

CRAC n° 11 (2026-2027)

4^e session de la XII^e législature

PARLEMENT WALLON

SESSION 2026-2027

COMPTE RENDU AVANCÉ*

Séance publique de commission

**Commission de la fonction publique
et des infrastructures sportives**

Lundi 28 septembre 2026

*Application de l'article 161 du règlement

Le compte rendu avancé ne peut être cité que s'il est précisé qu'il s'agit d'une version qui n'engage ni le Parlement ni les orateurs

Publication officielle du greffe du Parlement de Wallonie
Square Arthur Masson, 6
5012 Namur
compte.rendu@parlement-wallonie.be

Le compte rendu avancé constitue une reproduction provisoire des interventions des députés, des membres du Gouvernement et des autres orateurs. Il ne peut être cité que s'il est précisé qu'il s'agit d'une version qui n'engage ni le Parlement ni les orateurs.

Le compte rendu avancé est soumis à tous les orateurs qui peuvent retourner leurs corrections dans les 72 heures ouvrables. À défaut, ils sont censés se référer au texte reçu. Aucune modification de fond ne peut être apportée.

Une fois toutes les corrections examinées et éventuellement intégrées, le compte rendu est dit « compte rendu intégral » et remplace le compte rendu avancé sur le site web du Parlement de Wallonie.

Tous les comptes rendus sont disponibles sur le site **www.parlement-wallonie.be**, rubrique *Travaux parlementaires*, section *Publications*.

SOMMAIRE

OUVERTURE DE LA SÉANCE	1
ORGANISATION DES TRAVAUX	1
Examen de l'arriéré.....	1
AUDITIONS	1
La cybersécurité des services publics de Wallonie.....	1
Désignation d'un rapporteur.....	1
Intervenants : Mme la Présidente – M. Hervé Fiévet – M. Thierry Witsel.	
Audition de M. Guisse, Mme Roucou et Mme Quoilin, Secrétaire général a.i. du Service public de Wallonie (SPW), Directrice générale et Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital).....	1
Intervenants : Mme la Présidente – M. Stéphane Guisse, Secrétaire général a.i. du Service public de Wallonie (SPW) – Mme Isabelle Roucou, Directrice générale du Service public de Wallonie Digital (SPW Digital) – Mme Isabelle Quoilin, Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital).	
Audition de Mme Clouner, Directrice générale adjointe de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB).....	7
Intervenants : Mme la Présidente – Mme Phédra Clouner, Directrice générale adjointe de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB).	
Audition de Mme Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU).....	9
Intervenants : Mme la Présidente – Mme Kris Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU).	
Échange de vues.....	10
Intervenants : Mme la Présidente – Mme Jacqueline Galant, Ministre – Mme Éliane Tillieux – M. Chris Massaki Mbaki – M. Julien Liradelfo – M. Jean-Paul Bastin – Mme Veronica Cremasco – M. Stéphane Guisse, Secrétaire général a.i. du Service public de Wallonie (SPW) – Mme Isabelle Roucou, Directrice générale du Service public de Wallonie Digital (SPW Digital) – Mme Isabelle Quoilin, Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital) – Mme Phédra Clouner, Directrice générale adjointe de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB) – M. Jean-Luc Peeters, Directeur de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB) – Mme Kris Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU).	
Confiance au président et au rapporteur.....	36
REPRISE DE LA SÉANCE	36
INTERPELLATIONS ET QUESTIONS ORALES	36
Question orale de M. Stéphane Hazée à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « le cadrage budgétaire de la réforme des mandats ».....	36
Intervenants : Mme la Présidente – M. Stéphane Hazée – Mme Jacqueline Galant, Ministre.	
Question orale de Mme Éliane Tillieux à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « le suivi de l'examen du quatorzième rapport annuel du médiateur » ;	

Question orale de Mme Éliane Tillieux à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « la procédure intégrée de gestion des réclamations au sein du Service public de Wallonie (SPW) » ;

Question orale de Mme Éliane Tillieux à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « les tableaux de bord de suivi des recommandations du médiateur »..... 38

Intervenants : Mme la Présidente – Mme Éliane Tillieux – Mme Jacqueline Galant, Ministre.

Question orale de Mme Éliane Tillieux à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « le suivi de la cybersécurité des services publics wallons »..... 41

Intervenants : Mme la Présidente – Mme Éliane Tillieux – Mme Jacqueline Galant, Ministre.

Question orale de M. Thierry Witsel à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « l'impact de la sécheresse sur les terrains de football wallons »..... 43

Intervenants : Mme la Présidente – M. Thierry Witsel – Mme Jacqueline Galant, Ministre.

Question orale de M. Thierry Witsel à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « l'avenir de l'infrastructure de l'hippodrome de Wallonie après le désengagement régional »..... 44

Intervenants : Mme la Présidente – M. Thierry Witsel – Mme Jacqueline Galant, Ministre.

Question orale de M. Vincent Maillen à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « l'homologation des terrains synthétiques sans remplissage et la stratégie d'accompagnement »..... 45

Intervenants : Mme la Présidente – M. Vincent Maillen – Mme Jacqueline Galant, Ministre – Mme Éliane Tillieux.

Question orale de M. Thierry Witsel à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « la prévention des noyades par le recours à l'intelligence artificielle (IA) à la piscine de Spa »..... 46

Intervenants : Mme la Présidente – M. Thierry Witsel – M. Vincent Maillen – Mme Éliane Tillieux – Mme Jacqueline Galant, Ministre.

Question orale de Mme Sophie Fafchamps à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « le soutien régional au projet de développement du stade du Royal Football Club de Liège (RFCL) »..... 48

Intervenants : Mme la Présidente – Mme Sophie Fafchamps – Mme Jacqueline Galant, Ministre.

ORGANISATION DES TRAVAUX (SUITE)..... 48

Interpellations et questions orales transformées en questions écrites..... 48

Interpellations et questions orales retirées..... 48

LISTE DES INTERVENANTS..... 50

ABRÉVIATIONS COURANTES..... 51

COMMISSION DE LA FONCTION PUBLIQUE ET DES INFRASTRUCTURES SPORTIVES

Présidence de Mme Sophie Fafchamps, Présidente

OUVERTURE DE LA SÉANCE

- La séance est ouverte à 14 heures 1 minute.

Mme la Présidente. – La séance est ouverte.

ORGANISATION DES TRAVAUX

Examen de l'arriéré

Mme la Présidente. – L'ordre du jour appelle l'examen de l'arriéré de notre Commission. Quelqu'un souhaite-t-il prendre la parole sur celui-ci ?

Personne. Merci.

AUDITIONS

La cybersécurité des services publics de Wallonie

Mme la Présidente. – L'ordre du jour appelle les auditions sur la cybersécurité des services publics de Wallonie.

Désignation d'un rapporteur

Mme la Présidente. – Nous devons désigner un rapporteur. Quelqu'un a-t-il une suggestion à faire ?

La parole est à M. Fiévet.

M. Hervé Fiévet (MR). – Je propose M. Maillen comme rapporteur.

Mme la Présidente. – La parole est à M. Witsel.

M. Thierry Witsel (PS). – Je propose Mme Tillieux comme corapporteuse.

Mme la Présidente. – À l'unanimité des membres, M. Maillen et Mme Tillieux sont désignés en qualité de rapporteurs.

Audition de M. Guisse, Mme Roucou et Mme Quoilin, Secrétaire général a.i. du Service public de Wallonie (SPW), Directrice générale et Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital)

Mme la Présidente. – La parole est à M. Guisse.

M. Stéphane Guisse, Secrétaire général a.i. du Service public de Wallonie (SPW). – Mesdames et Messieurs les Députés, Madame la Ministre, Mesdames et Messieurs, je vous remercie de nous entendre aujourd'hui sur un sujet devenu essentiel pour toute administration publique.

Je précise que je vais parler d'abord, puis je céderai la parole à mes collègues, Mmes Roucou et Quoilin. Nous allons nous partager le temps de parole. Nous avons un PowerPoint qui peut être affiché en même temps.

Mme la Présidente. – C'est donc un PowerPoint commun pour tout le SPW : M. Guisse, Mme Roucou et Mme Quoilin. Cependant, je devrai tout de même reprendre la parole entre chaque personne pour vous la donner. Par ailleurs, je vous informe que le PowerPoint a déjà été envoyé aux députés via la plateforme.

La parole est à M. Guisse.

M. Stéphane Guisse, Secrétaire général a.i. du Service public de Wallonie (SPW). – Pour commencer, je vais vous préciser le cadre dans lequel je m'exprime. À l'époque de la cyberattaque, je n'occupais pas encore la fonction de Secrétaire général *ad interim*. J'étais directeur général de SPW Finances, donc je n'ai pas participé à la gestion opérationnelle de la crise, mais je n'en étais pas loin, je dois le confirmer.

Avant d'entrer dans le vif du sujet, je vais confirmer le vécu de la cyberattaque que j'ai ressenti ; je m'exprime ici à titre personnel. Je voudrais insister sur le fait que nous n'avons pas eu de destruction de données. Ce sont des choses que l'on a parfois entendues, mais je peux vraiment m'engager formellement sur le fait qu'aucune donnée de l'administration wallonne n'a été détruite. À ce stade, je n'ai pas de preuve, de certitude qu'il y a eu vol de données. Je vais être tout à fait prudent, puisque c'est clair que des données mettent parfois un certain temps à réapparaître sur le *dark web* ou ailleurs, mais je peux jurer sur l'honneur que, en ce qui me concerne, je n'ai

pas vu de preuve que des données massives du SPW ont été exfiltrées et exploitées.

Mon intervention, compte tenu de ma première remarque, portera dès lors sur la responsabilité institutionnelle du SPW aujourd'hui, sur les enseignements qui ont été tirés et sur la manière dont la cybersécurité est désormais intégrée dans la gouvernance de notre administration. La crise cyber, vécue par le SPW en 2025, a constitué un événement majeur, c'est indéniable. Elle a rappelé avec force combien nos missions publiques sont aujourd'hui dépendantes du numérique, mais elle a également démontré que la cybersécurité ne peut plus être aujourd'hui considérée comme une question exclusivement technique. Elle est devenue un sujet de gouvernance, de continuité des missions publiques, de gestion des risques et de responsabilité collective.

L'une des premières leçons de cette crise est qu'une cyberattaque devient immédiatement une crise institutionnelle. On l'a vécu en quelques jours, c'était un grand témoin tout à fait compréhensible : lorsqu'un système informatique est affecté, les conséquences dépassent largement le périmètre des équipes techniques. Ce sont potentiellement des aides qui ne peuvent plus être liquidées, des dossiers qui ne peuvent plus être traités, des informations qui deviennent inaccessibles, des services publics entiers qui ne peuvent plus être rendus dans les délais attendus.

La question n'est donc pas uniquement de protéger des infrastructures numériques, c'est de garantir ni plus ni moins la continuité du service public. C'est pourquoi la cybersécurité doit aujourd'hui être envisagée comme un élément constitutif de la qualité du service public. Dans la relation que nous avons, nous, au comité stratégique avec le Gouvernement wallon, c'est un bloc à part entière de gestion de nos activités.

Le deuxième enseignement que nous tirons de cette crise est qu'aucune direction, aucun expert et aucune technologie ne peut assumer seule cette responsabilité. Pendant longtemps, les organisations ont parfois considéré la cybersécurité comme une responsabilité essentiellement technique. L'expérience de ces dernières années montre qu'une telle approche n'est plus suffisante.

La cybersécurité est devenue une responsabilité collective et partagée. Le SPW Digital, en particulier, apporte une expertise spécialisée ; il construit et exploite les capacités de protection, de détection et de réponse. Les directions générales métiers doivent connaître leurs processus critiques, identifier leurs dépendances et participer à l'analyse de leurs risques. Les organes de gouvernance doivent arbitrer les priorités et les moyens. Les managers doivent intégrer la sécurité dans leur gestion quotidienne. Les agents eux-mêmes constituent une ligne de défense essentielle. Le Gouvernement wallon, enfin, fixe les priorités stratégiques et les

moyens nécessaires. Cette approche collective constitue aujourd'hui l'un des fondements de notre stratégie.

Une autre leçon importante est que le risque zéro n'existe pas et n'existera jamais. Cette réalité concerne aussi bien les administrations publiques que les entreprises privées ou les infrastructures critiques. L'enjeu n'est donc pas de prétendre supprimer tout risque, mais d'être capable d'identifier les risques, de les évaluer, de les hiérarchiser, de réduire ceux qui peuvent l'être et d'assumer explicitement ceux qui demeurent. Autrement dit, il s'agit de gouverner le risque. Cette capacité de gouvernance est devenue l'une des composantes essentielles de la maturité cyber.

Ce qui a changé depuis la crise, c'est que, depuis 2025, le SPW a progressivement structuré cette gouvernance. La sécurité de l'information s'inscrit désormais dans un cadre formalisé, avec des responsabilités clairement identifiées et des mécanismes de suivi qui permettent de piloter les progrès réalisés. Une gouvernance spécifique de la sécurité de l'information a ainsi été mise en place. La sécurité est désormais suivie au niveau stratégique, tactique et opérationnel, comme mes deux collègues vont vous en parler, et les priorités sont consolidées dans un programme coordonné à l'échelle du SPW tout entier. Cette approche vise à assurer une amélioration continue et mesurable.

Les progrès réalisés sont importants. Soyons néanmoins lucides et humbles : nous partons d'un niveau de sécurité qui est faible, il faut le reconnaître, et nous avons un retard important à rattraper. De plus, la cybersécurité n'est jamais achevée. Les menaces, les technologies, les obligations réglementaires et les attentes des citoyens évoluent en permanence. Notre défi consiste à atteindre et maintenir dans la durée un niveau de vigilance et d'investissement cohérent avec les risques auxquels nous sommes exposés.

À cet égard, la mise en œuvre de NIS 2 – on va en parler assez bien aujourd'hui après-midi – constitue un cadre structurant important. Elle nous pousse à objectiver notre maturité, à démontrer nos progrès et à inscrire la cybersécurité dans un mécanisme d'amélioration continue.

Avant de céder la parole à ma collègue Isabelle Roucou, je conclurai mon intervention par un message simple : la crise de 2025 a constitué un moment particulièrement important pour le SPW. Elle a rappelé l'importance stratégique de la cybersécurité et a démontré la nécessité d'une responsabilité collective. Aujourd'hui, notre responsabilité collective n'est pas de prétendre au risque zéro, mais de nous préparer, de nous améliorer continuellement et de garantir que le SPW demeure capable d'assurer ses missions essentielles au bénéfice des citoyens wallons.

Je vais maintenant céder la parole à Mme Isabelle Roucou, directrice générale du SPW Digital depuis une bonne année, qui va vous présenter plus concrètement la manière dont cette transformation a été structurée et les capacités mises en place depuis la crise.

Mme la Présidente. – La parole est à Mme Roucou.

Mme Isabelle Roucou, Directrice générale du Service public de Wallonie Digital (SPW Digital). – Monsieur le Secrétaire général, Madame la Présidente, Madame la Ministre, Mesdames et Messieurs les Députés, je vous remercie de nous donner l'occasion de présenter l'évolution de la cybersécurité au sein du Service public de Wallonie. Je souhaite aujourd'hui concentrer mon intervention sur ce que nous avons construit depuis la crise de 2025. Par ailleurs, je tiens à préciser que je n'étais pas encore en charge du SPW Digital à cette époque.

Aujourd'hui, l'enjeu n'est plus de regarder dans le rétroviseur, mais de comprendre comment une organisation publique transforme une crise en capacité durable de résilience. Un an après la restauration du système d'information, le sujet est la construction progressive d'un dispositif de cybersécurité plus mature, plus structuré et plus durable dans le temps. Cette démarche s'inscrit dans le cadre de la stratégie de sécurité de l'information du SPW et de la préparation aux exigences de NIS 2.

Pendant longtemps, la cybersécurité a été abordée principalement sous un angle technique. L'objectif consistait essentiellement à empêcher des attaques. Aujourd'hui, cette vision purement technique n'est plus suffisante. Les cyberattaques sont devenues une réalité permanente pour toutes les organisations, tant publiques que privées.

Dans ce contexte, la question n'est plus de savoir si une tentative d'intrusion surviendra, mais comment l'organisation que nous sommes est capable de l'anticiper, de la détecter et d'en limiter les impacts, et de poursuivre ses missions essentielles malgré la perturbation qui pourrait être créée par cette crise. C'est précisément ce que l'on appelle la cyberrésilience. Cette approche est au cœur des référentiels actuels de cybersécurité et des exigences NIS 2. Elle repose sur une vision plus globale qui combine gouvernance, connaissance de ses actifs, gestion des risques, protection, détection, réponse aux incidents et à la continuité d'activité.

Le véritable changement de paradigme est donc le suivant : la sécurité n'est plus uniquement une affaire d'outils et de spécialistes, elle doit devenir – elle devient d'ailleurs – une capacité organisationnelle à part entière, qui doit être pilotée dans la durée – à court terme, à moyen terme et certainement à long terme –, qui doit être financée de manière pérenne et qui doit être portée collectivement par l'ensemble de l'administration. Dans

cette logique, le SPW a engagé, depuis 2025, un vaste programme de transformation destiné à construire progressivement les capacités nécessaires à une cyberrésilience durable. Je vais vous en présenter ici les cinq capacités qui ont le plus évolué depuis la crise.

La première capacité, c'est gouverner la cybersécurité. Une des premières étapes a consisté, après la crise, à mettre en place un cadre de pilotage durable. La cybersécurité ne peut pas reposer uniquement sur des experts techniques. Elle doit être portée par une gouvernance claire, capable de définir des priorités, d'arbitrer des risques, de coordonner des actions et d'assurer un suivi de résultats. Depuis 2025, le SPW a progressivement mis en place des organes stratégiques, tactiques et opérationnels de gouvernance du futur système de management de la sécurité de l'information, le fameux SMSI.

Cette gouvernance rassemble les acteurs stratégiques, le Costra, les responsables métiers et IT dans des comités de direction et les responsables opérationnels. Cette gouvernance structure leurs échanges afin de permettre un pilotage cohérent de la sécurité à l'échelle de l'ensemble du SPW. C'est une évolution fondamentale et elle l'est parce qu'elle consacre un principe simple : la cybersécurité n'est pas uniquement de la responsabilité du SPW Digital, mais elle devient une responsabilité collective et partagée entre les métiers et le SPW Digital.

Un programme sécurité transversal pour le SPW a également été mis en place depuis 2025. Ce programme rassemble toutes les initiatives, projets et programmes de sécurité de l'information menés au SPW. La coordination est assurée par le SPW Digital. Les priorités et les objectifs sont validés dans les organes de gouvernance adéquats précités. Il est important également de mieux connaître nos risques et nos actifs. Pour protéger efficacement une organisation, encore faut-il savoir précisément ce que l'on souhaite et ce que l'on doit protéger.

Depuis un an, un travail important a été réalisé pour renforcer la connaissance du patrimoine numérique du SPW, améliorer l'identification des actifs critiques et développer une vision plus précise des dépendances entre les systèmes, les applications et les missions de service public. Parallèlement, une démarche structurée de gestion des risques est en cours de déploiement. L'objectif est de disposer progressivement d'une vision partagée des risques majeurs afin d'orienter les investissements et les priorités là où ils produisent le plus de valeur. Cette approche permet également de sortir d'une logique intuitive pour entrer dans une logique de décision fondée sur l'analyse, la mesure et l'objectivation des risques.

La troisième capacité, qu'il s'agit également de mettre en place et sur laquelle nous travaillons, est de protéger durablement le patrimoine numérique. Au-delà

de la gouvernance et de l'analyse des risques, il a fallu renforcer concrètement des fondations du système d'information. Depuis 2025, de nombreux travaux ont été réalisés afin d'améliorer progressivement le niveau de protection des infrastructures et des applications.

Ils concernent notamment :

- travailler sur la modernisation des composants devenus obsolètes ;
- renforcer des mécanismes de sécurité ;
- généraliser des mises à jour de sécurité ;
- réduire progressivement des vulnérabilités identifiées ;
- intégrer des exigences de sécurité dans le cycle de vie des applications.

Cet effort est particulièrement important, car le SPW gère un patrimoine numérique construit sur plusieurs décennies, caractérisé par une forte diversité technologique, par un niveau d'obsolescence parfois élevé et des investissements historiquement davantage orientés vers le développement de nouveaux services plutôt que vers leur maintien à niveau dans la durée.

Le défi consiste à améliorer simultanément la sécurité, la modernisation et la soutenabilité du système d'information. Ce travail est souvent invisible pour l'utilisateur ou le citoyen. Pourtant, il constitue l'une des conditions essentielles pour réduire durablement les risques et renforcer la robustesse générale de l'administration.

Il s'agit également de renforcer la quatrième capacité qui est d'investir dans les capacités humaines. Lorsque l'on parle de cybersécurité, on pense souvent aux technologies, mais ce n'est pas suffisant. Les incidents trouvent très fréquemment leur origine dans des comportements humains, des erreurs ou des habitudes inadéquates.

C'est pourquoi nous avons également engagé un programme de sensibilisation destiné aux différents publics du SPW : les dirigeants, les managers de première ligne, les profils techniques et les agents. Ainsi, une plateforme pérenne de sensibilisation est désormais déployée, sur laquelle des tests se font régulièrement. L'objectif de ces travaux n'est pas de transformer chaque agent en un expert en cybersécurité. L'objectif est plus simple : l'aider à développer des réflexes communs de vigilance et de cyberhygiène.

La résilience d'une organisation repose aussi sur des milliers de décisions quotidiennes prises par les hommes et les femmes qui composent cette organisation.

Enfin, la cinquième capacité sur laquelle nous avons beaucoup travaillé est de détecter et de réagir plus rapidement. La sécurité moderne ne repose pas uniquement sur la prévention ; elle repose aussi sur sa capacité à identifier rapidement un incident et à agir avant qu'il ne produise des conséquences importantes.

Depuis la crise, le SPW a progressivement structuré des capacités permanentes de surveillance, d'analyse et de traitement des incidents de sécurité. Cette évolution permet aujourd'hui une meilleure visibilité sur les événements de sécurité et une capacité accrue de réaction lorsqu'une situation anormale est détectée.

L'objectif poursuivi est simple : réduire le délai entre l'apparition d'un incident et sa prise en charge. Plus une organisation détectera rapidement un problème, plus elle sera capable d'en limiter les impacts. La détection et la réaction deviennent ainsi des fonctions permanentes de notre Service public, et non plus des activités exceptionnelles mobilisées uniquement en période de crise.

Le cadre NIS 2 est essentiel dans notre démarche. Il apporte un référentiel commun. Il permet d'évaluer la maturité de manière objective. Il aide à identifier les écarts et permet également de prioriser les actions à entreprendre.

Le SPW a engagé un vaste exercice d'évaluation de sa maturité en cybersécurité, afin d'identifier précisément ses forces, ses lacunes et ses priorités futures. Cet exercice permettra de disposer, d'ici fin 2026, d'une vision objectivée de la situation de maturité actuelle, et d'élaborer ensuite une trajectoire pluriannuelle, priorisée et budgétée.

Il est important de rappeler que la conformité NIS 2 n'est pas une question de conformité administrative ou documentaire. Elle vise avant tout à démontrer qu'une organisation est capable de piloter ses risques, de mettre en œuvre des mesures adaptées et d'améliorer continuellement son niveau de maîtrise. C'est précisément la démarche engagée aujourd'hui au SPW.

Mesdames et Messieurs les Députés, la crise de 2025 a mis à l'épreuve notre capacité à restaurer les services avec un niveau minimal de sécurité. Notre ambition d'aujourd'hui et pour l'avenir est de construire cette administration résiliente : une administration capable d'anticiper des risques, de détecter des incidents, de réagir rapidement, de maintenir ses missions essentielles et d'apprendre continuellement de son expérience. En d'autres termes, nous passons progressivement d'une logique de restauration à une capacité durable de cyberrésilience. Cette trajectoire est engagée, structurée et pilotée, mais elle n'est pas encore terminée.

Comme toutes les grandes organisations publiques, nous devons encore poursuivre nos efforts pour réduire progressivement la dette technologique accumulée, harmoniser nos pratiques, renforcer certaines compétences et atteindre le niveau de maturité attendu dans le cadre de la directive NIS 2. Notre responsabilité collective est désormais de poursuivre cet effort dans la durée afin de garantir la continuité, la fiabilité et la

confiance nécessaires à l'exercice des missions publiques dont le SPW a la charge.

Je vous remercie tous de votre attention. Mme Quoilin va désormais vous faire un rapide retour d'expérience sur la gestion de la crise cyber de 2025.

Mme la Présidente. – La parole est à Mme Quoilin.

Mme Isabelle Quoilin, Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital). – Madame la Présidente, Mesdames et Messieurs les Députés, M. Stéphane Guisse a présenté le cadre institutionnel dans lequel le SPW inscrit aujourd'hui la cybersécurité. Mme Isabelle Roucou a ensuite expliqué les capacités mises en place depuis la crise, ainsi que les travaux qui restent à mener. Pour ma part, je vais revenir sur la gestion concrète de la crise cyber d'avril 2025. Mon objectif est de présenter les principales décisions prises ; l'organisation de la restauration ; les difficultés rencontrées et les enseignements que l'administration en a tirés.

La gestion générale de la crise relevait de la secrétaire générale du SPW. Elle était appuyée par un collègue chargé de la coordination des équipes informatiques et par moi-même en qualité de coordinatrice stratégique. J'ai donc participé au dispositif dès les premières heures, à l'interface entre les équipes techniques, les responsables métiers, les autorités administratives, le Gouvernement et les partenaires institutionnels. Je ne présenterai pas les éléments relevant de l'enquête, les vulnérabilités ou les dispositifs techniques dont la divulgation pourrait affecter la sécurité actuelle du SPW. Je me concentrerai sur l'organisation administrative et opérationnelle de la réponse.

Pour comprendre les décisions prises, il est utile de rappeler que la cybersécurité poursuit trois objectifs essentiels : protéger la confidentialité des informations ; garantir leur intégrité et assurer la disponibilité des systèmes et des données nécessaires aux missions de service public.

Le 3 avril 2025, une vulnérabilité importante a été détectée. Une solution technique alternative a été activée pour se protéger face à cette vulnérabilité, et le niveau de vigilance des équipes a été renforcé. Le 15 avril, suite à cette vigilance renforcée, une intrusion à haut risque a été identifiée. L'outil concerné par cette intrusion a été immédiatement isolé et le Centre pour la cybersécurité Belgique – le CCB – a été mobilisé, comme le prévoient les obligations NIS 2.

Le 17 avril, les analyses menées par les équipes informatiques et le CCB ont confirmé l'existence d'une intrusion majeure. Face au risque de propagation, une décision lourde, mais nécessaire, a été prise à 19 heures ce même jour : isoler l'ensemble du système d'information, c'est-à-dire le couper d'internet, et activer les dispositifs régionaux de gestion de crise.

Cette décision visait avant tout à préserver l'intégrité du système d'information et la confidentialité des données. Son impact était cependant considérable, puisqu'elle entraînait l'indisponibilité de nombreux services dont la restauration allait ensuite être organisée progressivement et de manière sécurisée. Nous avons néanmoins pu préserver la disponibilité des systèmes industriels gérés par le Service public de Wallonie Mobilité et Infrastructures, comme les barrages, les tunnels et les feux de signalisation. En l'absence d'indices de compromission, ils ont été isolés du reste du système informatique et maintenus en fonctionnement dégradé.

Dès le 18 avril – le lendemain, donc –, la restauration est organisée autour d'un principe simple : ne reconnecter un système qu'après l'avoir analysé et sécurisé, et après avoir évalué le risque associé.

La première phase a consisté à coordonner la réponse, confiner la menace, reconstruire les composants indispensables qui avaient été compromis et rétablir les accès sécurisés. Il a également fallu établir dans l'urgence une première cartographie des actifs numériques du SPW.

La deuxième phase a permis de reconnecter progressivement les applications et infrastructures les plus critiques pour les métiers, ce que nous appelons « les joyaux de la couronne ». Pour chacun d'eux, il a fallu analyser les dépendances, évaluer les risques, définir les mesures de protection nécessaires, puis réaliser les travaux de sécurisation avant toute remise en service. Mi-juin, à la fin de cette phase, environ 80 % des activités impactées étaient totalement ou partiellement rétablies.

Une troisième phase a permis de généraliser les mesures de sécurité de base et de retirer certains composants obsolètes, et de poursuivre les reconnections sur la base d'un niveau de sécurité objectivé. Mi-septembre, à la fin de cette phase, 95 % des activités initialement touchées étaient rétablies.

Enfin, une phase de consolidation a permis de traiter les dernières situations résiduelles, ainsi que les applications nécessitant un hébergement ou des adaptations plus profondes. La restauration complète du système a été achevée le 22 décembre 2025.

Avec le recul, cette séquence rappelle une réalité importante : aujourd'hui, aucune organisation publique ou privée ne peut garantir qu'elle ne sera jamais victime d'une cyberattaque. La véritable question n'est donc pas de savoir si une attaque peut survenir, mais plutôt comment l'organisation réagit lorsqu'elle survient. Le 17 avril 2025, nous avons fait le choix de privilégier la protection du système d'information et des données, même au prix d'une interruption importante de service. Cette décision a eu des conséquences immédiates pour

l'administration, mais elle a permis de contenir la menace.

Sans cette mesure d'isolement, nous risquons une propagation beaucoup plus importante de l'attaque. Davantage de systèmes auraient pu être compromis ou rendus inutilisables. Des données sensibles auraient pu être exposées ou détruites, et une partie beaucoup plus importante de notre patrimoine informatique aurait pu devoir être reconstruite. Les délais de restauration, les coûts et les impacts sur les missions de service public auraient alors été considérablement plus élevés. En d'autres termes, l'objectif du 17 avril n'était pas d'éviter toute conséquence. Il était d'éviter le pire. Avec le recul, c'est précisément ce que cette décision a permis de faire.

Des difficultés ont quand même été rencontrées. J'en reprends ici les quatre principales. Elles montrent qu'en situation de crise, la difficulté n'est pas seulement technique : il faut aussi décider vite, coordonner de nombreux acteurs et maintenir l'effort dans la durée.

La première difficulté concernait la connaissance de notre système d'information. Les informations disponibles évoluaient rapidement. Il fallait préciser les relations entre les infrastructures, les applications et les métiers qu'elles soutenaient. Cette analyse devait être ensuite traduite en éléments suffisamment clairs pour soutenir les décisions.

La deuxième difficulté était la priorisation. Tous les services présentaient une utilité, mais ils ne pouvaient pas être restaurés simultanément. Il a fallu donc définir des critères communs, examiner les impacts humains, juridiques, financiers et opérationnels de chaque indisponibilité. Les priorités ont été établies avec les métiers, puis réévaluées en fonction des risques techniques et les progrès de la restauration.

La troisième difficulté concernait la coordination. La gestion de la crise mobilisait les équipes techniques, les directions métiers, les autorités administratives et gouvernementales, ainsi que plusieurs partenaires institutionnels. Il fallait organiser la circulation de l'information, clarifier les responsabilités, maintenir un cadre de décision commun alors que la situation continuait d'évoluer.

Enfin, la durée de la crise a constitué une difficulté en elle-même. Les équipes ont été mobilisées pendant plusieurs mois et même, à certaines périodes, sept jours sur sept, 24 heures sur 24. Il a fallu organiser les relais, maintenir les compétences nécessaires et préserver la capacité de travail dans la durée.

Nous avons aussi tiré cinq enseignements majeurs – repris dans le rapport postcrise de l'administration – de cette crise. Le premier enseignement concerne l'organisation de crise. Les rôles et responsabilités, circuits de décision et modalités de remplacement doivent être définis avant la crise. Ils doivent également

être testés. Le cadre régional de gestion de crise qui préexistait a également apporté un soutien utile. Il doit être complété par des plans de continuité et de reprise adaptés aux différents scénarios.

Le deuxième enseignement porte sur la connaissance des activités critiques. Pour décider rapidement, l'administration doit connaître ces processus essentiels, les applications qui les soutiennent, leurs dépendances techniques et les solutions de repli disponibles. Cette connaissance permet de déterminer plus rapidement les priorités de restauration.

Le troisième enseignement concerne la répartition des responsabilités. Le SPW Digital fournit les infrastructures, l'expertise et les capacités techniques. Les directions métiers identifient leurs activités critiques, évaluent les conséquences d'une interruption et préparent les modalités de continuité. Les autorités administratives et gouvernements arbitrent les priorités et les moyens.

Le quatrième enseignement porte sur la communication. En période de crise, il faut déterminer qui produit l'information, qui la valide et à qui elle est destinée, par quels canaux elle est diffusée. Des moyens alternatifs doivent être prévus lorsque les outils habituels ne sont plus disponibles.

Enfin, le cinquième enseignement concerne le suivi du retour d'expérience. Les constats établis après la crise ont été traduits en recommandations. Celles-ci doivent être affectées à des responsables, planifiées, financées et suivies. C'est ce qui permet de vérifier que les difficultés constatées donnent effectivement lieu à des adaptations.

C'est précisément ce qui a été fait. Ces enseignements, ainsi que les recommandations techniques formulées par les experts qui nous ont accompagnés, que ce soit le CCB ou la Detect and Response Team de Microsoft ont, d'une part, inspiré la vision institutionnelle présentée par M. Guisse et, d'autre part, été intégrées et priorisées dans le Programme de sécurité de l'information du SPW, dont Mme Roucou vient de vous présenter les avancées majeures.

Mme la Présidente. – La parole est à M. Guisse.

M. Stéphane Guisse, Secrétaire général a.i. du Service public de Wallonie (SPW). – Pour conclure cette intervention du SPW – je ne vais pas être très long –, vous avez compris par nos interventions successives que c'est une crise multifacettes.

Ce que je retiens comme enseignement principal, c'est que les cybercrises ne se limitent plus uniquement à la technique. C'est tout un ensemble de facteurs qui fait que l'on peut y résister et en tirer les enseignements.

La crise est derrière nous, on peut le dire. Depuis le mois de décembre 2025, on peut la considérer comme clôturée. Or, il est clair que les conséquences de cette crise ne sont pas terminées, puisque nous avons modifié substantiellement la façon de faire les choses, de la gouvernance du SPW. Je crois utile d'insister : nous ne promettons pas le risque zéro. C'est impossible, ce serait mentir. Vous le voyez dans l'actualité, les attaques sont de plus en plus violentes, de plus en plus organisées. Nous avons des IA qui se liguent comme outil très puissant. Le grand travail que nous faisons, c'est de limiter l'impact en cas de crise et limiter les propagations possibles d'une attaque si quelqu'un rentre dans nos systèmes.

Si je devais clôturer cette intervention par une seule phrase : une cybercrise se traite par la technique, mais elle se surmonte par la gouvernance, la coopération et la préparation. Merci beaucoup.

Audition de Mme Clouner, Directrice générale adjointe de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB)

Mme la Présidente. – La parole est à Mme Clouner.

Mme Phédra Clouner, Directrice générale adjointe de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB). – Madame la Présidente, Mesdames et Messieurs les Députés, Madame la Ministre, merci de nous accueillir aujourd'hui.

Nous allons revenir sur certains éléments qui ont déjà été évoqués par les représentants du SPW. Ma présentation va se diviser en plusieurs parties. Dans un premier temps, nous allons présenter le contexte de la menace au niveau belge, au niveau international, mais aussi au niveau des administrations publiques. Ensuite, je reviendrai sur ce que le CCB offre et a offert comme services au SPW dans le cadre du traitement de cette crise. Nous reviendrons sur une rapide ligne du temps de la manière dont cela s'est passé, même si cela a déjà été expliqué par le SPW. Nous terminerons avec quelques informations sur la directive NIS 2.

Sur ce *slide*, vous voyez le nombre de notifications qui nous ont été reportées entre 2023 et 2026. Vous pouvez effectivement constater que de nombreux incidents nous sont rapportés, au CCB, en tant qu'autorité nationale de cybersécurité, et CSIRT national. Vous pouvez aussi constater qu'il y a une certaine augmentation à partir de fin 2024. Cela s'explique-t-il par l'entrée en vigueur de la directive NIS 2 ? Oui, bien évidemment.

Lorsque vous voyez ce paysage de la menace en 2025, qui n'a pas particulièrement changé en 2026, que constate-t-on ? Il y a effectivement des menaces

récurrentes qui touchent tous les secteurs. Comme il a été dit, le risque zéro n'existe pas et aucun secteur n'est épargné, ni au niveau belge, ni au niveau européen, ni au niveau international. On voit essentiellement des comptes compromis, des rançongiciels et des attaques DDoS. Les attaques DDoS, a priori, rendent les sites indisponibles, mais on ne s'introduit pas dans les systèmes.

Il y a également énormément de menaces d'ingénierie sociale. Je pense que vous avez été tous confrontés, d'une manière ou d'une autre, à des mails de *phishing*, des messages WhatsApp ou ce genre de choses, qui vous encouragent à partager vos informations pour accéder à vos comptes ou à vos informations bancaires.

Les secteurs les plus ciblés de la NIS 2 sont les administrations publiques, qui représentent à peu près 22 % des notifications que nous avons eues en 2025, avec le transport et la santé. Nous avons des exemples relativement fréquents au niveau d'hôpitaux touchés par des attaques.

On voit aussi que les cybercriminels utilisent des vulnérabilités connues pour s'introduire dans les systèmes. Les vecteurs d'attaque sont les courriels d'hameçonnage, comme le *phishing* – d'après l'ENISA, l'Agence européenne de cybersécurité, c'est à peu près 60 % de l'origine des cyberattaques encore actuellement –, l'exploitation de vulnérabilités connues et l'utilisation d'identifiants de comptes compromis.

Au niveau des incidents significatifs par secteur, entre octobre 2024 et juin 2026, cela illustre très bien le fait que les administrations publiques sont des cibles privilégiées de ces attaques.

Au niveau des interventions – parce que ce n'est pas parce qu'il y a des notifications au niveau du CCB que le CCB intervient nécessairement –, entre janvier et août 2026, il y a eu 31 interventions de la part du CCB sur les administrations publiques.

Comme je le disais, il n'y a pas que la Belgique, en définitive, qui est touchée par des cyberattaques touchant plus spécifiquement les administrations publiques, puisque l'ENISA a constaté que ce phénomène se produisait au niveau européen et au niveau des différents États membres pour 2025. Nous avons la même tendance jusqu'à présent en 2026.

À côté, le CCB offre un certain nombre de services aux administrations – je reviendrai là-dessus –, dont la diffusion de notifications de menaces aux différents publics cibles du CCB. Ces publics cibles sont bien les administrations publiques également.

Que fait le CCB ? C'est l'Agence nationale de cybersécurité, nous sommes aussi le CSIRT national. Ce que fait le département CERT, qui est aujourd'hui représenté par M. Peeters, c'est de surveiller et

d'analyser les cybermenaces et vulnérabilités, de traiter les cyberincidents au niveau national et, sur demande, d'apporter une assistance aux organisations concernées, en analysant, en contenant l'incident, en atténuant les effets de l'incident et en éradiquant les éléments qui sont liés à cette attaque. C'est exactement ce que nous avons fait dans le cadre de la cybercrise du SPW.

À côté, nous avons aussi un département qui a pour objectif d'analyser la menace de manière très détaillée, qui peut toucher la Belgique, les différents secteurs. Sur base de cette analyse, nous diffusons des avis sur les menaces, des alertes sur les menaces et aussi sur la manière de contrer ces menaces. Ce que l'on fait aussi, le cas échéant, c'est aider les autorités judiciaires dans le cadre d'une information ou d'une instruction judiciaire. Par contre, ce que l'on ne fait pas – c'est important –, c'est prendre des décisions à la place des services, victimes de cyberattaques, c'est reconstituer l'infrastructure de l'organisation victime et c'est assurer la gestion des réseaux et systèmes lors d'un incident ou d'une crise.

Très rapidement, les services du CCB, dont le SPW peut bénéficier, ce sont les alertes sur les menaces. Le SPW en a bénéficié, puisque le CCB avait envoyé une alerte sur la menace. On propose aussi un service, qui est offert par notre CERT, de réponse aux incidents. À côté, on offre aussi tout un tas de services qui sont liés à la mise en place de la directive NIS 2.

Beaucoup de sensibilisation et d'information pour les différents publics cibles du CCB, que ce soient les citoyens, les organisations publiques et privées, et utilisables aussi par le SPW, un référentiel de sécurité pour aider justement les organisations, essentiellement NIS 2, à prioriser les mesures de sécurité à mettre en place et aussi la possibilité pour les organisations d'identifier leur niveau de maturité avec des outils que l'on met à disposition.

Très rapidement, mais cela a déjà été expliqué, voici la ligne du temps par rapport à cet incident. En effet, le 3 avril, Ivanti et Mandiant ont divulgué une vulnérabilité, et le CCB a envoyé une alerte précoce aux organisations belges concernées, dont le SPW. Le 15 avril, le CCB contacte le SPW, qui confirme en effet que des activités suspectes sont signalées et une réponse conjointe à l'incident est lancée. Dès le 15 avril, le CCB était présent pour mettre à disposition du SPW toutes ces ressources afin de comprendre déjà la problématique, de confiner et de mitiger au maximum l'impact de la crise.

L'incident a été élevé au niveau d'incident national. À la suite d'une recommandation du CCB, comme cela a été expliqué, le SPW a interrompu la connexion à internet pour éviter que cela se propage et que cela fasse des dégâts encore plus importants. La Région wallonne a engagé l'assistance additionnelle de Microsoft. Le CCB a été désigné en qualité d'expert judiciaire pour

cet incident. En mai 2025, la synthèse exécutive a été faite et le rapport final a été remis le 27 mai 2025.

Quelques recommandations générales dans ce type d'incident, et qui ont déjà été évoquées par les représentants du SPW, c'est renforcer durablement la capacité interne de cybersécurité. Oui, il faut mettre en place une équipe interne spécialisée, dotée de personnel formé et capable de prévenir, de détecter et de gérer les incidents de cybersécurité. Le plan du SPW montre effectivement que l'on est dans cette optique. Des procédures, des réponses aux incidents doivent également être adaptées afin de garantir la préservation des preuves numériques. Cela fait partie du plan du SPW également. Il faut traiter la dette technique comme un enjeu de sécurité structurelle. Ce type d'incident illustre vraiment les risques qui sont liés à des systèmes obsolètes ou non supportés, ou des outils, ce genre de choses. La sécurité doit être vraiment intégrée dans tout le cycle de vie de la technologie. C'est ce qui est en train d'être mis en place par le SPW.

Il faut aussi investir correctement dans la cybersécurité, car nous avons vu qu'une cyberattaque peut avoir des conséquences vraiment très importantes. Comme a été dit, le risque zéro n'existe pas. D'une manière ou d'une autre, il faut pouvoir faire face à ce genre de choses. La cybermenace devient de plus en plus importante, à tel point que la Commission européenne a publié une directive, puis une deuxième, pour protéger les secteurs critiques et essentiels au niveau européen. Cela montre bien à quel point la problématique de la cybersécurité est de plus en plus prégnante. De plus, vu la digitalisation et les nouveaux types de menaces qui apparaissent, cela ne va pas changer du tout, bien au contraire. C'est donc sur ce genre de directives et de lois que l'on mise aussi énormément d'espoir pour augmenter le niveau de cybersécurité et de cybermaturité des États membres et de leurs entités essentielles, dont le SPW fait partie.

Ce que toute entité NIS 2 doit faire, c'est s'enregistrer – c'est fait –, mais aussi prendre des mesures de gestion des risques en matière de cybersécurité – c'est en cours au niveau du SPW. C'est aussi tout ce qui a trait à la gestion des incidents, ainsi qu'aux obligations et responsabilités du management, qui constituent un élément très important de la directive NIS 2. Enfin, il y a une obligation de collaboration avec les autorités compétentes ; nous en avons la preuve parfaite dans le cadre de cet incident.

Parmi les mesures de cybersécurité à mettre en œuvre, qui sont indiquées à la fois dans la directive et dans la loi, figurent effectivement l'analyse des risques, la gestion des incidents, la continuité des activités, la sécurité de la chaîne d'approvisionnement et d'autres choses de ce genre. À côté de cela, la loi NIS 2 demande aussi une identification des organisations publiques, dont fait partie le SPW. C'est en cours. Actuellement, une liste a été fournie avec les informations concernant

les administrations publiques de la Région wallonne qui doivent être reprises dans le *scope* de la directive NIS 2. Nous sommes en train de finaliser – en parfaite consultation avec la Région wallonne – l'établissement de cette liste.

Voilà où nous en sommes. C'est un processus qui est en cours au niveau des différentes Régions et entités fédérées. Outre cela, il y a aussi une obligation de coopération au niveau national entre les pouvoirs publics et l'autorité nationale de cybersécurité, ce qui est mis en place actuellement. Nous avons aussi un accord de collaboration avec l'Agence du numérique dans le cadre de la mise en place de la Cyber Response Team, qui aura aussi un effet sur la sécurisation d'entités NIS 2 au niveau de la Région wallonne. Voilà qui conclut mon intervention dans les temps.

Mme la Présidente. – Merci beaucoup. M. Peeters ne souhaite pas prendre la parole, puisqu'il semble que Mme Clouner s'est exprimée en son nom également.

Mme Phédra Clouner, Directrice générale adjointe de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB). – Oui, je suis désolée, j'ai parlé pour tout le monde.

Mme la Présidente. – Quand un homme cède son temps de parole à une femme, je le souligne et l'apprécie toujours beaucoup.

(Rires)

Vous avez bien réparti les interventions, puisqu'il y avait deux femmes pour un homme. C'était une petite boutade.

Nous allons passer à Mme Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU). Avant cela, chers collègues, je vous informe que nous pourrions passer à huis clos si cela s'avère nécessaire, par exemple si des données trop sensibles sont exposées ou si l'on estime que nous ne pouvons pas nous exprimer librement avec les micros.

Audition de Mme Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU)

Mme la Présidente. – La parole est à Mme Derkoningen.

Mme Kris Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU). – Comme expliqué, je viens de la Federal Computer Crime Unit. Je vais parcourir ce que fait la FCCU et notre position au sein de la police fédérale, puis j'expliquerai le cadre et les limites de mon intervention d'aujourd'hui, les constats tirés du dossier et quelques recommandations par rapport à celui-ci. Enfin, je terminerai par une petite conclusion.

Par rapport aux compétences de la police intégrée au niveau des faits de cybercriminalité, on a, d'une part, la police locale, où la plupart des plaintes sont déposées, et qui mène des enquêtes autonomes pour des dossiers dits plus « simples » et plutôt locaux, et tout ce qui est *cyber-enabled crimes*. Je pense à des faits de *phishing* et tout ce qui est plus large – *ransomware*, *hacking* – et qui ne sera jamais fait au niveau local. Dans certaines polices locales, on a aussi une LCCU, local computer crime unit, mais c'est dans les plus grandes zones de police.

D'autre part, on a la police fédérale et les quatorze regional computer crime units – RCCU – qui sont organisés au niveau des arrondissements judiciaires, au sein des directions décentralisées. Ils vont mener des enquêtes autonomes, surtout au niveau des *ransomwares*. On a aussi la FCCU, qui va également mener des enquêtes judiciaires. C'est plus particulier, comme des faits de *cyber-dependent* : *hacking*, *data sabotage*. La victime doit être une infrastructure critique, ce qui a fait en sorte que ce qui s'est passé au SPW est arrivé chez nous comme dossier. On fait également une coordination dans toute la Belgique pour tout ce qui est relatif à la complexité des dossiers. On va superviser, également l'aspect international, au niveau de la FCCU.

Par rapport à ce dossier, l'objectif n'est pas d'analyser le dossier judiciaire, mais d'identifier plutôt les axes d'amélioration permettant de réduire les risques de futurs incidents majeurs.

Il me paraît important de préciser que la police intégrée n'est pas l'autorité chargée de définir des politiques de prévention ou les standards de cybersécurité. Ce n'est pas notre rôle. Cette mission relève du Centre pour la cybersécurité Belgique. Les quelques recommandations que je formule aujourd'hui sont issues des constats réalisés dans le cadre du traitement du dossier et doivent donc être considérées sous cet angle. Je ne prétends pas du tout être exhaustive par rapport à l'expertise du CCB et de ce que les collègues du SPW ont déjà mis en place entre-temps.

Au niveau des constatations, il faut peut-être dire aussi que la police a été impliquée très tardivement dans le cadre de ce dossier. Un point d'attention pour le futur, c'est de nous impliquer assez vite dans ce genre de dossier. Pour la gouvernance informatique, on a remarqué une gestion fortement décentralisée dans le cadre du dossier. Ce qui a comme conséquence qu'il est difficile de disposer d'une vision complète de l'environnement informatique. Parmi les éléments constatés figure une forte autonomie des différentes directions générales dans la gestion de leur système informatique. Cela peut conduire à l'utilisation de technologies différentes et rendre plus difficile l'obtention d'une vue globale de l'environnement informatique ainsi que la gestion centralisée de sécurité.

La gestion des incidents est une deuxième constatation. On a remarqué une difficulté de réaction face à un incident majeur comme cela a eu lieu. Cette absence de pilotage centralisé à l'égard de certains aspects de la sécurité peut compliquer cette gestion d'un incident majeur lorsqu'il est difficile d'obtenir rapidement une vision d'ensemble. Les possibilités de réaction sont également plus limitées – on l'a remarqué de notre côté.

Dans l'architecture du réseau, on a vu une exposition de certains systèmes : la présence d'adresses IP internes routables mérite une attention particulière, puisqu'elle peut permettre, sur le plan technique, certaines communications directes entre l'internet et les éléments internes d'un réseau.

Autre constatation, c'est la gestion des systèmes et applications, mais cela a déjà été expliqué avant. C'est donc aussi l'utilisation d'outils obsolètes et le vieillissement des technologies. On a aussi remarqué des retards dans certaines mises à jour. Il s'agit d'un constat régulièrement rencontré dans de nombreuses organisations. Cela souligne l'importance d'une gestion continue du cycle de vie des systèmes.

Les petites recommandations à notre niveau – en entendant les présentations des collègues, je peux vous indiquer qu'elles ont déjà été mises en route – sont les suivantes :

- définir un plan de sécurité commun pour l'ensemble du SPW afin de disposer d'un plan contraignant susceptible d'assurer une cohérence minimale entre les différentes entités ;
- obtenir une vue globale de l'infrastructure, comprenant une cartographie complète de celle-ci ainsi que les outils utilisés par chaque direction. Cela nous semble tout de même important. Cette visibilité constitue un prérequis à toute gestion efficace de la sécurité ;
- renforcer la gestion du cycle de vie des systèmes – comme cela a déjà été expliqué à plusieurs reprises. Les mises à jour ou un remplacement progressif des technologies obsolètes au travers d'une planification structurée nous semblent très importants ;
- procéder à la création ou au renforcement d'une structure centralisée chargée de la sécurité. Cela permettrait d'améliorer la cohérence des décisions et les suivis des risques à l'échelle de l'ensemble du SPW ;
- inclure une clause relative à la cybersécurité dans les contrats publics. Nous avons ainsi également pensé aux marchés publics. Il s'agit d'une autre piste de solution à suivre dans le futur.

J'ai repris sur cette diapositive les principaux axes de renforcement. Je souhaiterais tout de même souligner l'importance d'impliquer rapidement les services spécialisés en cas d'incident cyber. Plus nous sommes associés tôt, plus nous pouvons comprendre ce qu'il

s'est passé, adopter un soutien adapté – surtout en ce qui concerne la police – et préserver les traces utiles pour notre enquête par la suite. C'est un des principaux enseignements que je peux partager avec vous aujourd'hui concernant l'intervention de la police.

Échange de vues

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Je veux d'abord remercier l'administration, les représentants du SPW Digital, le Centre pour la cybersécurité Belgique ainsi que la police fédérale pour leur présence et pour la qualité des éclairages qui viennent d'être apportés. Cette audition est importante. Elle permet de poser les faits, de mesurer le chemin parcouru et d'identifier lucidement ce qui doit encore être consolidé. Elle traduit aussi mon engagement envers le Parlement de communiquer en toute transparence les informations nécessaires à l'exercice de son contrôle démocratique, tout en protégeant les éléments techniques ou opérationnels dont la divulgation pourrait fragiliser la sécurité de nos systèmes.

Sur un sujet devenu majeur pour l'administration wallonne comme pour l'ensemble des services publics, la transparence et la sécurité ne s'opposent pas. Elles doivent être conciliées de manière responsable. Nous devons replacer cette discussion dans son contexte. La menace cyber n'est plus un risque périphérique. Elle s'inscrit dans une situation géopolitique internationale instable, marquée par des opérations d'influence, des actes de sabotage numérique, l'usage de rançongiciels et des attaques visant aussi bien les entreprises que les services publics. Les incidents récents, qui ont touché plusieurs administrations et opérateurs publics en France, montrent qu'aucun État, même doté de moyens importants, n'est à l'abri. Pour une administration comme le Service public de Wallonie, investir dans la cybersécurité n'est donc ni un luxe ni une dépense de défense isolée. Cela revient à protéger la continuité de l'action publique, les données des citoyens et la capacité même de l'administration à remplir ses missions.

La réponse wallonne ne part pas de rien. Un travail avait déjà été engagé ces dernières années, notamment avec la création du SPW Digital et la volonté de mieux structurer le pilotage numérique de l'administration. Toutefois, il faut aussi le dire clairement : en matière de cybersécurité, aucun dispositif n'est jamais définitivement suffisant. La menace évolue très vite. Elle touche aujourd'hui toutes les organisations – publiques comme privées – en Belgique, en Europe et partout dans le monde. Les administrations sont devenues des cibles à part entière. Dès lors, la vraie

question n'est plus de savoir si une organisation peut être attaquée, mais quand elle le sera, avec quelle intensité et surtout dans quel état de préparation elle se trouvera au moment d'y faire face.

C'est dans ce contexte que la crise d'avril 2025 doit être comprise. Comme cela a été expliqué en commission le 12 mai 2025 et rappelé aujourd'hui, la décision rapide d'isoler les systèmes était une décision nécessaire. Elle a permis de contenir le risque et d'éviter que la situation ne s'aggrave.

Ensuite, la remise en service a été organisée par priorités, en fonction de la criticité des missions, des dépendances techniques et du niveau de sécurité requis. Oui, le redémarrage a été progressif. Oui, il a été plus long que certains services. Cependant, restaurer vite ne peut pas signifier reconnecter sans contrôle.

Depuis lors, le Gouvernement a validé une stratégie de cybersécurité pour l'ensemble du SPW, mobilisé des moyens complémentaires et engagé un programme permanent de sécurisation. Les recommandations formulées après la crise, notamment par le CCB et par les experts mobilisés, ont été analysées, priorisées et traduites en actions suivies.

L'objectif n'est pas de promettre qu'aucune attaque ne se produira jamais. Ce serait irresponsable. L'objectif est de réduire les risques, de mieux les détecter, de réagir plus vite, de restaurer plus solidement et de limiter autant que possible l'impact d'un incident futur.

Les prochains mois doivent convertir l'évaluation de maturité en cours qui a été évoquée par le SPW en un plan d'action concret, priorisé et financé. Il faudra poursuivre la mise en œuvre des recommandations, renforcer les plans de continuité, préparer des exercices, réduire l'obsolescence et revenir vers le Gouvernement avec une trajectoire objectivée.

Cette trajectoire doit aussi intégrer deux enjeux désormais indissociables de la cybersécurité : la souveraineté numérique – c'est-à-dire notre capacité à maîtriser notre dépendance critique, nos données et nos choix technologiques – et l'intelligence artificielle, qui peut renforcer la détection et l'analyse, mais crée également de nouveaux risques liés aux données, aux modèles, aux usages et aux fournisseurs.

Notre ambition est claire : une administration plus numérique, mais aussi plus robuste, plus souveraine et capable de rester opérationnelle en situation de crise. Je vous remercie et je voulais remercier une nouvelle fois l'administration dans son ensemble.

Mme la Présidente. – La parole est à Mme Tillieux.

Mme Éliane Tillieux (PS). – Tout d'abord, je voudrais remercier toutes les personnes présentes dans cette salle pour cette séance d'auditions. Je voudrais noter que c'est la première depuis le lancement de cette

législature. Il a fallu attendre deux ans avant de réellement débattre autrement qu'entre parlementaires. On avait eu une fois l'École d'administration publique, mais c'était dans le cadre d'une présentation sur l'école et les budgets.

Ici, on est dans un tout autre contexte, celui d'un événement externe, d'un incident qui a frappé de plein fouet l'administration publique, qui a beaucoup ému. Je pense que tous ceux qui ont exercé des responsabilités ont cette crainte et cette angoisse chaque jour que la porte soit forcée, et a fortiori des systèmes informatiques.

Ils recèlent énormément de données, et surtout, ils conditionnent le fonctionnement de l'organisation et la poursuite et la continuité de l'activité. Derrière, il y a un public qui attend un service. S'il y a défection, on ne peut plus rendre le service comme attendu. C'est d'autant plus important, Mme la Ministre a dit aussi que ces auditions sont importantes.

C'est dommage d'avoir dû attendre presque un an et demi depuis l'événement pour enfin marquer le coup et se pencher sur la question de l'organisation et toutes les questions qui peuvent se poser par rapport à ce type d'incident.

L'administration, rappelons-le, a subi une attaque. Elle n'est pas l'auteure, elle est victime de cette réalité. Je voudrais remercier toutes les personnes présentes aujourd'hui qui représentent l'administration. Ils n'étaient peut-être pas en poste à ce moment-là, mais ils exercent des responsabilités aujourd'hui, ou ils ont connu d'un peu plus loin cette réalité opérationnelle et viennent l'expliquer, y compris jusqu'à un ressenti personnel. Cela me fait chaud au cœur de savoir comment vous appréciez ce parcours, ce trajet parfois un peu complexe et difficile de se mettre en ordre de marche par rapport à ce type d'événement difficile.

On sait que l'on est en difficulté tous les jours : guerres hybrides, des flottes fantômes et des cyberattaques. Les failles belges face aux menaces font encore l'objet d'une série d'articles, pointant le fait que des sites majeurs sont des cibles potentielles – je m'adresse peut-être plus à la police –, comme nos hôpitaux, qui ont été assez régulièrement la cible d'attaques et encore dernièrement, mais aussi les administrations et nos Parlements. Dès lors, notre démocratie peut aussi être la cible de cyberattaques. L'administration de notre Parlement relevant toutefois d'une tout autre organisation, nous n'en parlerons pas dans notre Commission.

On a suivi ce dossier depuis les premières attaques et l'on a multiplié les questions parlementaires. Madame la Ministre, on est revenu à diverses reprises sur l'évolution de la résolution de cette crise. On a demandé des auditions dès 2025 parce qu'une crise de cette ampleur mérite davantage qu'un simple échange

politique entre majorité et opposition. Selon nous, il est nécessaire d'entendre ceux qui ont géré l'incident et ceux qui connaissent l'état de nos systèmes ainsi que les autorités chargées de cybersécurité et d'enquête, ce qui dépasse largement le contexte wallon.

On n'est pas ici pour interférer sur l'enquête judiciaire, comme plusieurs d'entre vous l'ont rappelé ; là n'est pas du tout la question. On ne recherche pas les responsables de cette situation. On essaie de comprendre comment on peut mieux s'organiser pour répondre à ce risque qui devient quotidien. On est ici pour comprendre ce qu'il s'est passé, ce qui était prêt ou qui ne l'était pas. Quels enseignements ont été tirés ? Notre administration dispose-t-elle aujourd'hui des moyens humains, techniques et budgétaires nécessaires pour assurer durablement la continuité du service public ?

Par rapport aux auditions, j'ai un peu l'impression que l'on a passé sous silence cette question des moyens. On a bien vu les enseignements et les recommandations. Or, pour nous, parlementaires, ce qu'il est intéressant de savoir, c'est si nous avons les moyens de nos ambitions. J'aurai quelques questions à vous poser à cet égard.

On a deux écueils à éviter : tout rendre public ou, à l'inverse, invoquer systématiquement la confidentialité, ce qui reviendrait à empêcher notre contrôle parlementaire. Je rappelle les circonstances dans lesquelles on se trouve ici aujourd'hui : on exerce notre contrôle parlementaire.

Le Parlement n'a pas vocation à connaître les éléments opérationnels qui permettent de reproduire l'intrusion, l'architecture détaillée du réseau, les indicateurs de compromission toujours sensibles et les éléments protégés par le secret de l'enquête. Cela ne concerne toutefois pas la gouvernance – et vous en avez largement parlé –, les effectifs, les budgets, l'existence ou non de dispositifs de continuité, la chronologie des décisions, les recommandations formulées au Gouvernement, les besoins identifiés, les décisions d'investissement et les modalités générales de coopération entre les institutions.

J'imagine que, depuis lors, des partenariats se sont soit créés de manière spontanée à la suite de l'attaque, soit sont entrevus afin de mieux coopérer demain – cela a été mis en évidence à plusieurs reprises – sur la rapidité de réaction et sur la réaction univoque et non pas disparate.

Comme Mme la Présidente l'a rappelé, il est tout à fait possible, comme le prévoit le règlement, que la réunion de notre Commission se déroule à huis clos à certains moments afin de permettre d'échanger avec une nécessaire confidentialité, par exemple, liée au secret de l'instruction.

Madame la Ministre, quel mécanisme peut désormais garantir au Parlement un suivi régulier des

suites de cette crise et de l'enquête, en distinguant clairement ce qui peut être communiqué publiquement, ce qui pourrait l'être à huis clos et ce qui demeurer complètement couvert par le secret de l'enquête et qui ne concerne pas le contrôle parlementaire ? C'est très important parce que l'on n'en a pas fini et que c'est quelque chose qui va perpétuellement être un risque.

Dès lors, nous pourrions adopter un mécanisme qui permettrait aux parlementaires d'être aussi rassurés. Cela pourrait prendre la forme d'une espèce de tableau de bord sur ce qui avance : y a-t-il des nouveautés ou y a-t-il de nouveaux modèles ? En effet, avec l'intelligence artificielle, les risques sont multipliés. Pourrions-nous avoir une espèce de *reporting* automatisé ou bien qui est suscité par l'un ou l'autre événement ? Il s'agirait d'une manière de venir expliquer spontanément au Parlement et non d'attendre un an et demi plus tard qu'une demande d'explication soit adressée par le Parlement. Il s'agirait d'alerter de manière spontanée : « Il y a eu un nouveau risque, nous avons bien réagi. Voilà ce que nous avons mis en place ». On pourrait avoir une espèce de suivi qui permet d'être rassuré ou de mieux comprendre ce que vous vivez au niveau du SPW.

Il est vrai que cette attaque d'avril de l'année dernière n'était pas la première alerte puisque, en octobre 2024 déjà, une attaque DDoS avait frappé Wallonie.be et que, à l'époque, Madame la Ministre, vous aviez annoncé différents renforcements. Ce n'étaient d'ailleurs pas les premières attaques puisque la Chambre – où j'ai siégé durant la législature précédente – avait également fait l'objet d'attaques assez fortes, mais avait pu résister, grâce à une prise de conscience très forte des personnes impliquées, des systèmes et de ceux qui s'activaient sur la sécurité. Heureusement, un plan de sécurité avait été pensé précédemment, ce qui a permis d'éviter de complètement bloquer le système. Ce n'est pas évident, mais c'est une évolution inéluctable.

Des articles publiés après l'intrusion d'avril ont évoqué une forte obsolescence du parc applicatif, l'absence d'un plan de rétablissement pleinement opérationnel et l'absence, avant l'attaque, d'un centre opérationnel de sécurité, en tout cas équivalent au dispositif 24/7 déployé ensuite. Ces affirmations journalistiques ne peuvent pas être assimilées à un audit officiel. C'est ce que nous avons lu dans la presse. Dès lors, les auditions d'aujourd'hui constituent précisément l'occasion de confirmer, de corriger ou de nuancer toutes ces affirmations. Quel diagnostic précis de cybermaturité existait avant l'attaque d'avril 2025 ? Comment étions-nous organisés ? Compte tenu de cette situation, quels écarts entre ce diagnostic et ce qui existe aujourd'hui ont pu être comblés ? Qu'est-ce qui a fait qu'aujourd'hui on est plus mature ?

Le 1^{er} avril 2025, le directeur général du SPW Digital quitte le service et, quelques jours plus tard, l'incident intervient. La presse avait également signalé

le départ antérieur de l'inspectrice générale en charge de l'exploitation. Ainsi, deux figures du SPW Digital manquent à l'appel au moment où justement cette cyberattaque survient. Je ne voudrais pas déduire que les vacances de fonction ont causé ni aggravé l'attaque, pas du tout. Cependant, il serait intéressant de savoir quelle était la chaîne de responsabilités au moment de l'attaque. Qui disposait de l'autorité de décision ? Un dispositif intérimaire avait-il été mis en place ? Si des décisions étaient retardées faute de responsables à l'époque ? Quelles fonctions essentielles n'étaient pas pourvues ? Comment le Gouvernement a-t-il réagi en ces circonstances ?

La question du Disaster Recovery Plan – le plan de restructuration ou de reprise des activités – a été soulevée à de nombreuses reprises dans nos interventions au sein de cette commission. Aujourd'hui, il serait intéressant de savoir s'il y avait un dispositif de reprise, s'il existait concrètement.

Quelles applications étaient couvertes par ce plan ? A-t-il été testé ? Selon quels scénarios ? Des exercices avaient-ils eu lieu pour le tester ? Des dépendances techniques avaient-elles été identifiées ? Quels écarts ont été révélés par la crise ? Cette crise n'a-t-elle pas aussi permis d'en apprendre plus par rapport au plan qui avait été, le cas échéant, mis en place voici un an et demi ?

Mme la Ministre a indiqué qu'un centre opérationnel de sécurité fonctionne 24 heures sur 24, sept jours sur sept, depuis mai 2025. Ce service est chargé de surveiller, d'analyser et de traiter les incidents de cybersécurité en continu. Pourquoi ce niveau de surveillance n'existait-il pas avant l'incident ? Depuis quand son besoin a-t-il été identifié ?

En termes de moyens humains, nous devrions pouvoir documenter quelles compétences sont disponibles en interne ou en externe. Nous comprenons bien qu'il n'est pas toujours évident de recruter les bons profils, qu'il faut parfois recourir à de l'expertise externe, mais rappelons que le statut est un élément qui peut parfois justement permettre d'attirer du personnel extérieur, qui peut se sentir rassuré d'avoir un avenir dans le même parcours professionnel. C'est important dans les orientations que prend aujourd'hui notre Gouvernement. Je vais passer à une liste de questions.

Monsieur Guisse, vous avez pris vos fonctions après la cyberattaque. Avez-vous eu un retour d'expérience formalisé ? Avez-vous eu une transmission de cette gestion de crise de la cyberattaque ? Bien sûr, vous étiez déjà impliqué au niveau de l'organisation de la direction du SPW, mais avez-vous eu un retour d'expérience plus formalisé qui identifiait des difficultés au niveau de la chaîne de commandement, de la gouvernance, de la remontée des alertes ou des délégations de décisions ? Avez-vous déjà eu un état des lieux au moment de votre arrivée ?

Quelles recommandations, en ce qui concerne l'organisation du SPW, avez-vous décidé de mettre en œuvre depuis votre prise de fonction ? Parmi les difficultés révélées par la crise, lesquelles considérez-vous aujourd'hui comme entièrement résolues ? Lesquelles sont en cours de traitement ? Lesquelles restent encore tout à fait ouvertes ?

À votre arrivée, avez-vous reçu un inventaire des besoins – humains, techniques et financiers – qui n'étaient pas rencontrés en matière de cybersécurité ? On sait que les moyens manquent toujours par rapport aux ambitions. C'est d'autant plus vrai en matière d'IT. Quelles demandes supplémentaires par rapport à cet état des lieux avez-vous depuis lors adressées au Gouvernement ?

Nous l'avons vu dans les *slides* qui ont été présentées, mais je voulais vous poser la question du rôle respectif du Secrétariat général, du SPW Digital, du Centre régional de crise et des différentes directions générales. Cela a-t-il été clarifié ? Il me semble que, dans vos *slides*, vous avez tenté de répondre à cette question. Avez-vous quelque chose à ajouter ? Cela s'adresse aussi à Mme Roucou.

Existe-t-il désormais une chaîne de décision formalisée testée dans le cadre d'exercices de crises ? Le comité stratégique reçoit-il désormais régulièrement un tableau de bord relatif aux risques cyber, à la dette technologique, aux vulnérabilités et à la continuité de l'activité ? Quels indicateurs permettent aujourd'hui au Secrétariat général de vérifier que les recommandations formulées après avril 2025 sont effectivement mises en œuvre. La cyberattaque a-t-elle entraîné une modification durable des priorités budgétaires et organisationnelles du Service public de Wallonie ? En clair, disposez-vous aujourd'hui des moyens nécessaires pour garantir dans la durée les investissements effectués depuis 2025 ou identifiez-vous encore un déficit ? Les enseignements tirés de la crise ont-ils été formalisés dans un document de type retour d'expérience ou plan d'action ? Une version non sensible pourrait-elle être communiquée à notre Parlement ?

Si vous deviez identifier trois décisions que vous pourriez prendre aujourd'hui pour éviter qu'une future intrusion ne provoque à nouveau un confinement aussi général, quelles seraient ces trois décisions à prendre immédiatement ?

J'ai des questions pour Mme Roucou. Merci aussi à vous pour votre présence. Je voudrais remercier, à travers vous, le travail accompli par les équipes du SPW Digital ; si vous pouviez transmettre nos remerciements pour leur dévouement depuis la cyberattaque.

Vous avez donc été désignée manageuse de transition du SPW Digital le 12 juin 2025, après l'attaque. On sait que vous connaissiez toutefois déjà

l'environnement du SPW Digital. La presse indique d'ailleurs que vous y aviez exercé une mission externe en matière de cybersécurité et que vous auriez alerté sur certains risques avant la fin de votre mission, en décembre 2024. Aujourd'hui, il est important que vous puissiez confirmer, préciser ou corriger ces informations. Dès lors, nous pourrions, au travers de votre audition, comprendre à la fois ce qui était déjà identifié avant l'attaque, et ce qui a été découvert ensuite et qu'il a été décidé de corriger au moment de votre retour, après la crise. L'objectif n'est pas de demander un jugement politique, mais d'obtenir un diagnostic factuel sur les risques, les moyens, la gouvernance et les mesures encore nécessaires.

Par ailleurs, la presse indique aussi que SPW Digital aurait souhaité la prolongation de votre mission après décembre 2024. Est-ce exact ? Si oui, pour quelle raison ? À votre retour comme manageuse de transition en juin 2025, quels étaient pour vous les trois principaux problèmes structurels identifiés au SPW Digital ? Parmi ces trois principaux problèmes structurels, lesquels étaient déjà connus avant l'attaque et lesquels ont été révélés ou aggravés par la crise ? Quel était l'état réel du plan de reprise après sinistre et de la surveillance permanente des systèmes avant et après avril 2025 ? Le Centre opérationnel de sécurité actuellement en place était-il déjà prévu avant l'attaque ?

Sur le plan des applications du SPW, quelle est aujourd'hui l'ampleur de la dette technologique ? On sait que beaucoup d'applications étaient obsolètes au moment de l'intrusion. Quel calendrier est prévu pour résorber cette dette technologique ? De la même manière, si vous aviez trois décisions à prendre aujourd'hui pour éviter qu'une future intrusion provoque à nouveau un confinement aussi général, quelles seraient, selon vous, les trois décisions à prendre immédiatement et à quel niveau ?

Pour Mme Quoilin, que j'ai rencontrée et connue dans d'autres fonctions antérieurement au SPW. Vous connaissez bien le SPW pour avoir dirigé le SPW Économie, Emploi et Recherche pendant plusieurs années avant de rejoindre le SPW Digital. Vous êtes actuellement coordinatrice sécurité. Pourriez-vous expliquer un peu plus avant quel rôle vous avez joué pendant la crise ? Par rapport à vos deux précédents collègues qui se sont exprimés, vous étiez en place au niveau du SPW Digital lorsque les événements se sont déroulés. Pourriez-vous distinguer les systèmes réellement compromis des applications arrêtées préventivement ?

Comment avez-vous pu classer les applications pour déterminer l'ordre de restauration ? Existait-il, avant l'incident, une cartographie suffisamment complète des dépendances entre applications ? Quels enseignements avez-vous tirés en ce qui concerne la gestion des comptes privilégiés, des accès, de la journalisation et de la détection ? Le plan de reprise qui existait a-t-il

fonctionné comme prévu ? Sinon, quels écarts l'incident a-t-il mis en évidence ?

À quelle date les outils de surveillance 24 heures sur 24 et sept jours sur sept actuellement opérationnels ont-ils été décidés, commandés, mais, surtout, effectivement mis en place ? Quel est, selon vous, le degré de couverture actuel du centre opérationnel de sécurité ? Quelle famille d'applications anciennes constitue encore la principale difficulté de sécurisation ?

Pour vous qui êtes aussi au cœur du SPW Digital, quels besoins en personnel cyber demeurent aujourd'hui non pourvus ? Comme pour vos prédécesseurs, si vous deviez identifier trois décisions à prendre pour éviter une future intrusion et un confinement général, quelles seraient-elles ?

Je passe au Centre pour la cybersécurité Belgique ; je vous remercie pour votre exposé, qui était assez rapide, mais très intéressant. Je vous remercie aussi pour les actions que vous menez, que ce soit au travers de l'incident du SPW ou de manière générale. À quel moment précis votre centre a-t-il été alerté de l'incident du SPW ? Avez-vous vous-mêmes lancé l'alerte ? En effet, je crois savoir qu'il y a des allers-retours. À quel moment votre centre a-t-il été impliqué en termes opérationnels ?

Vous qui avez cette expertise, comment pourriez-vous qualifier, de manière générale et sans révéler d'éléments sensibles, la complexité et la gravité de l'incident ? La décision de couper les connexions internet de l'ensemble du Service public de Wallonie était-elle, selon votre analyse, proportionnée par rapport aux informations disponibles à ce moment ? Le niveau de préparation de l'administration avant l'incident correspondait-il aux pratiques que votre centre recommande pour une administration de cette taille et de cette criticité ? Je ne vous demande pas une appréciation politique, mais plutôt des critères objectifs par rapport à un référentiel dont vous pourriez disposer.

Quels dispositifs considérez-vous comme indispensables pour une administration telle que le Service public de Wallonie ? J'imagine que cela inclut un centre opérationnel de sécurité 24 heures sur 24 et sept jours sur sept, un plan de continuité, un plan de reprise testé, la gestion des vulnérabilités et un inventaire des actifs. Une partie de la réponse est dans vos *slides*, mais souhaitez-vous apporter des ajouts ? Le Service public de Wallonie disposait-il de chacun de ces dispositifs à un niveau suffisamment opérationnel avant l'incident d'avril 2025 ? Avez-vous les moyens de le savoir, puisque ce n'est peut-être pas votre rôle ?

Quelles catégories de recommandations le centre a-t-il formulées après l'incident ? Là aussi, une partie de la réponse se trouve dans les *slides*, mais vous pourriez mettre en avant les recommandations les plus urgentes. Avez-vous aujourd'hui connaissance de

recommandations majeures qui resteraient en suspens et encore à exécuter ?

De manière générale, comment voyez-vous l'évolution de la coopération entre votre centre et les entités fédérées ? L'entrée dans l'univers NIS 2 modifie-t-elle concrètement le niveau d'exigence auquel une administration – et, a fortiori, le Service public de Wallonie – doit répondre ? Quelles sont aujourd'hui, un an et demi plus tard, les principales menaces qui doivent le plus préoccuper les grandes administrations publiques ? En d'autres termes, les choses ont-elles encore évolué depuis ? Voyez-vous l'intelligence artificielle modifier concrètement le volume ou le degré de sophistication des attaques ? Le niveau de maturité du Service public de Wallonie correspond-il aux standards attendus d'une administration publique ? Y a-t-il un niveau plus élevé en raison de cet incident ? Si des écarts subsistent, à quel niveau se situent-ils ?

En ce qui concerne la Federal Computer Crime Unit de la police fédérale, sans aborder le contenu de l'enquête, pouvez-vous nous expliquer les rôles respectifs de votre service, du Centre pour la cybersécurité Belgique et de l'organisation victime quand une intrusion majeure survient ? Comment ces organisations se coordonnent-elles ? Y a-t-il des recommandations à formuler à cet égard ? Il y avait des éléments dans vos *slides*, mais peut-être avez-vous une réponse plus directe à donner. À partir de quel moment une réponse à un incident technique devient-elle également une enquête judiciaire ? Qu'est-ce qui fait que l'on bascule d'une réponse technique à apporter à une attaque au lancement d'une enquête judiciaire ? Comment préserver les preuves sans ralentir excessivement la restauration des services ? Quelles sont les informations qu'une administration victime devrait absolument conserver immédiatement après la détection d'une intrusion ?

Selon vous, les administrations publiques sont-elles aujourd'hui davantage visées par des attaques de nature criminelle, politique ou géopolitique que des sites privés ? Constatez-vous une professionnalisation des groupes cybercriminels ? L'utilisation croissante de l'intelligence artificielle modifie-t-elle la manière dont vous menez vos enquêtes ou la manière dont vous percevez les cyberattaques ? Comment améliorer les services communs et les échanges entre administrations, police et centres de cybersécurité avant qu'une crise se produise ? On a vu comment faire après, mais peut-on anticiper ? Si oui, comment ?

Je voudrais poursuivre avec une série de questions à Mme la Ministre, qui vont porter sur les choix et décisions du Gouvernement et non pas sur la responsabilité des agents de l'administration.

Madame la Ministre, à votre arrivée en juillet 2024, il y avait-il un état des lieux précis de la cybersécurité du SPW. Avez-vous reçu de la part de votre

prédécesseur, c'est-à-dire Mme De Bue, un état des lieux de la situation avec des risques considérés comme prioritaires ? À quelle date avez-vous été informée des difficultés en ce qui concerne le plan de reprise, la surveillance 24 sur sept ou l'obsolescence d'applications ? Quelle décision avez-vous prise entre votre entrée en fonction et avril 2025 pour y répondre ?

Par rapport au management du SPW Digital, quand avez-vous été informée du départ annoncé du précédent directeur général ? Pourquoi la continuité de la direction n'a-t-elle pas été assurée avant son départ, le 1^{er} avril ? Qui assumait formellement la responsabilité du SPW Digital en avril 2025 ? Y avait-il un dispositif d'intérim prévu, avec quelle délégation de décision ? Les auditions pourront-elles établir si cette situation de management a eu ou non un impact opérationnel ?

En termes de moyens humains, c'est important, combien de fonctions informatiques ou cybercritiques étaient vacantes en avril 2025 ? Combien le sont aujourd'hui ? En clair, avez-vous pu combler les déficits ? Les métiers de cybersécurité ou d'exploitation IT bénéficient-ils désormais d'exceptions haute priorité dans les politiques de remplacement ou de recrutement ? Quelle stratégie de fidélisation pouvez-vous mettre en place face à la concurrence du secteur privé ? Avez-vous évalué spécifiquement l'impact de la fin de la statutarisation, de la norme budgétaire de recrutement et des autres réformes des ressources humaines sur l'attractivité et la fidélisation des métiers IT et cyber au niveau du SPW ?

Les fonctions informatiques et de cybersécurité considérées comme critiques disposent-elles d'un régime de priorité ou de marche particulière de recrutement ? Combien de postes ont pu ainsi être ouverts ou remplacés depuis la crise ?

Au niveau budgétaire – il ne s'agit pas ici de faire tout le débat budgétaire, cela viendra en temps utile, mais un petit rappel –, quels montants le SPW Digital avait-il précisément demandés pour 2025 avant les arbitrages du Gouvernement ? Quels montants lui ont finalement été accordés à l'initial ? Pouvez-vous distinguer clairement pour 2025 et 2026 les crédits consacrés au fonctionnement informatique général de ceux spécifiquement affectés à la cybersécurité ? Sur les 8 millions d'euros exceptionnels attribués en 2025 au périmètre IT du SPW Digital, quel montant a été engagé et effectivement liquidé ? Quel éventuel solde reste aujourd'hui disponible ? Quelle est désormais la trajectoire budgétaire structurelle pour les années à venir, 2027, 2028, 2029, pour maintenir ces dispositifs dans la durée ? On a vu à plusieurs reprises, dans les *slides*, que la question de la durée et de la soutenabilité de la durée de ces moyens budgétaires est importante.

En termes d'externalisation, quel est le coût total de Microsoft DART et des autres expertises externes mobilisées pour l'incident et la restauration ? En clair,

qu'a coûté cet incident de manière externe par rapport aux moyens du SPW ? Quel transfert de compétences vers les équipes en interne est également prévu ? On sait que, pour les positions critiques, il est important de disposer non seulement des technologies, mais aussi des ressources humaines pour les gérer en interne.

Plus globalement, Madame la Ministre, disposez-vous désormais d'une estimation consolidée du coût de la crise avec les prestations externes, le matériel et les licences supplémentaires, la restauration, les retards administratifs, les renforts humains et les investissements qui ont dû être accélérés ? Quels enseignements issus de l'attaque reste encore à mettre en œuvre ?

Enfin, acceptez-vous de transmettre au Parlement un tableau de bord non sensible de la maturité cyber du Service public de Wallonie, avec les investissements, les effectifs, les incidents significatifs, les audits, les exercices et l'avancement de NIS 2 ? Ce serait évidemment rassurant pour l'ensemble des parlementaires de cette Commission.

Mme la Présidente. – La parole est à M. Massaki Mbaki.

M. Chris Massaki Mbaki (MR). – Je tenais vraiment à remercier l'ensemble des intervenants pour toutes les informations qu'ils ont pu nous communiquer.

Comme vous le savez, la cyberattaque d'avril 2025 a profondément perturbé le fonctionnement du Service public de Wallonie. Elle nous a surtout rappelé qu'une cyberattaque contre une administration ne touche pas uniquement des systèmes informatiques. Elle peut directement affecter la continuité du service rendu aux citoyens. Nous, en tant que politiques, c'est évident que, lorsque nous avons suivi la cyberattaque, même à travers les journaux, nous pouvions nous mettre directement à la place du citoyen et nous rendre compte à quel point nous avons très peu d'informations sur les données qui ont potentiellement fuité, qui ont pu potentiellement se retrouver dans les mains d'autres personnes mal intentionnées. C'est important que l'on puisse rassurer en tout cas la population. Monsieur Guisse, vous l'avez aussi très bien fait. D'entrée, c'est ce que nous retiendrons surtout de l'ensemble de vos prises de parole : pas de perte de données, et – vous le dites quand même avec une certaine nuance – jusqu'à preuve du contraire, qu'il n'y aurait pas de vol de données. Ce sont vraiment des informations importantes qui doivent être communiquées auprès du citoyen.

Alors, certains reviennent sur le temps d'attente pour mettre en place ces auditions. Nous, nous préférons surtout mettre en avant le travail qui a été effectué parce que, oui, nous aurions pu tenir des auditions plus tôt, mais la vraie question, c'est de se dire : était-il opportun de vous faire venir ici, au Parlement, alors que l'on était en pleine cyberattaque ? Clairement, non. Vous aviez

d'autres choses à faire et je crois que vous avez bien fait votre travail. Cela aurait été tout sauf responsable de vous faire venir.

Aujourd'hui, on est un an et demi après cette cyberattaque, et l'heure, pour nous, est surtout aux enseignements et aux perspectives pour l'avenir. Là-dessus, depuis – on en a parlé à travers les interventions –, au niveau de ce Parlement, on a pu discuter des différents moyens qui étaient donnés au niveau du SPW Digital et pour la cybersécurité. Des moyens importants ont été mobilisés et la gouvernance de la cybersécurité a été renforcée. Le SPW s'est également engagé dans une évaluation de sa maturité au regard de la directive NIS 2, dont les résultats consolidés sont attendus pour la fin de cette année. On a parlé aussi du timing pour le changement de la direction au niveau du SPW Digital. C'est pareil pour la directive NIS 2. Lorsqu'on fait justement certaines adaptations, on n'est jamais à l'abri qu'à ce moment-là on soit pris pour cible d'une éventuelle cyberattaque.

Je vais aller droit au but vers mes trois questions. Au-delà des moyens investis, quels indicateurs permettront concrètement au Gouvernement et au Parlement de mesurer l'amélioration de la cybersécurité du SPW dans les prochaines années ? Si la crise a montré l'importance du facteur humain, comment comptez-vous vous assurer que les agents, mais aussi les responsables et managers soient régulièrement formés et préparés à réagir en cas de nouvelles attaques ? Je souligne d'ailleurs que cette formation doit être récurrente et adaptée en fonction des différents profils.

Enfin, au niveau de l'intelligence artificielle – puisqu'on en parle beaucoup, nous avons fait la demande pour aussi rencontrer les homologues Digitaal Vlaanderen ; cela pourrait être aussi intéressant de comparer, de voir un peu ce qui se passe de l'autre côté. L'intelligence artificielle peut-elle devenir un outil supplémentaire pour les SPW, notamment pour détecter plus rapidement des anomalies ou des tentatives d'attaques ? Si oui, comment comptez-vous encadrer son utilisation afin qu'elle constitue réellement un outil de protection sans créer de nouvelles vulnérabilités ?

J'ai peut-être rajouté une petite question en dernière minute en me disant que, en tant que conseiller communal, ce serait aussi intéressant de savoir quelles sont les procédures lorsqu'il y a justement une cyberattaque qui se produit au niveau des communes.

Lorsqu'elle est attaquée, qui accompagne concrètement une petite commune wallonne qui n'aurait pas de responsable de la sécurité des systèmes d'information ni de véritable équipe cyber ? Pour nous, cela peut être intéressant d'avoir ces informations. Je vous remercie d'avance pour les réponses.

Mme la Présidente. – La parole est à M. Liradelfo.

M. Julien Liradelfo (PTB). – D’abord, je tiens à remercier les différents intervenants pour leurs explications. C’est un sujet assez technique, si je puis dire, un secteur complexe. On ne prétend pas être des experts. On a vécu une grave crise, et c’est important aussi de rappeler que, derrière cette attaque informatique, toute une série de choses, comme des paiements, des demandes de permis, ont été bloquées. Il y a des citoyens derrière qui attendaient des réponses. Des travailleurs du SPW eux-mêmes ont dû faire face à cette attaque. Je tiens évidemment à saluer une fois de plus leur travail. On sait que lorsque des crises pareilles arrivent, ce sont des moments difficiles et on peut heureusement compter sur le service public pour essayer d’arriver à un retour à la normale. On voit que l’on a eu besoin aussi de plusieurs services – j’ai d’ailleurs aussi une question pour la police fédérale.

Mais je soulignerai d’abord que la question des moyens humains et techniques n’a pas été abordée dans les différentes interventions. Madame la Ministre, pensez-vous aujourd’hui que nous avons les moyens humains, techniques et financiers nécessaires pour être préparés à de potentielles nouvelles crises de ce genre ?

Monsieur Guisse, avez-vous un bilan complet du retard provoqué par la crise, que ce soit en termes de dossiers retardés, de réencodage ou de productivité ? En fait, quelles conséquences concrètes cette crise a-t-elle eues sur les citoyens et les services ?

J’ai cru comprendre qu’aujourd’hui, c’était résolu à 100 % – sauf erreur, car il y a eu beaucoup d’informations. Pouvez-vous le confirmer ? Et dans le cas contraire, pouvez-vous nous dire ce qu’il reste à faire pour un retour à la normale à 100 % ?

J’avais une question concernant les consultants. On sait qu’en décembre 2025, le SPW Digital comptait environ 500 personnes, dont environ la moitié étaient consultantes. Peut-être pouvez-vous confirmer ce chiffre. Y a-t-il une réflexion, une procédure pour réinternaliser ces fonctions ? J’ai entendu tout à l’heure parler d’équipes spécialisées. Ces équipes spécialisées font-elles partie d’une stratégie de réinternalisation et de diminution du recours à des boîtes de consultants, eu égard à des secteurs stratégiques ? Faut-il continuer à passer par de la consultance avec des secteurs sensibles, ou y a-t-il un plan pour réinternaliser ces compétences ?

Tous les services qui ont été considérés comme critiques ont-ils été testés au moins une fois depuis la crise ? Et si ce n’est pas le cas, combien en reste-t-il à tester ? Dans quel pourcentage sommes-nous ?

Après l’attaque, plusieurs séries de recommandations ont été formulées, notamment par le CCB et Microsoft. Les recommandations que vous considérez comme les plus critiques ont-elles été appliquées ? Le CCB a-t-il lui-même vérifié leur mise en œuvre, ou cela repose-t-il principalement sur les informations fournies par le SPW ?

J’avais une question pour Mme Derkoningen. Vous avez parlé, à un moment, de gouvernance informatique. Vous avez dit que les services avaient une certaine autonomie, mais travaillaient avec des outils différents. Vous l’avez pointé comme un problème. Je voudrais savoir si, à l’inverse, le fait d’avoir tous les mêmes outils ne peut pas être une source de vulnérabilité. Parce que, si un service est attaqué et que tout le monde travaille avec les mêmes outils, n’est-ce pas aussi un risque, dans l’autre sens, d’être vulnérable aux mêmes attaques, par exemple ?

J’ai aussi une question concernant l’intelligence artificielle. On a tous l’impression que la réponse va être oui, mais, aujourd’hui, avec les avancées de l’intelligence artificielle, les attaques vont-elles être plus virulentes, plus violentes ? Vont-elles se multiplier ? Quelle est la part aujourd’hui ? Avez-vous un pourcentage d’attaques qui sont directement menées avec des IA ? Est-ce 100 % le cas ? L’IA est-elle en train d’aggraver la situation en termes d’attaques informatiques ?

Concernant la procédure : qui contacte qui quand il y a une attaque ? Avez-vous été sollicité ou est-ce vous qui proposez vos services directement, sachant l’ampleur de l’attaque ? Je voulais savoir quelle procédure était mise en place à ce niveau.

Mme la Présidente. – La parole est à M. Bastin.

M. Jean-Paul Bastin (Les Engagés). – Madame la Présidente, M. Christophe Bastin a dû s’absenter et je le remplace ici aujourd’hui. Tout d’abord, merci pour les différentes présentations et le travail qui a été fait, que ce soit avant, durant ou après la cyberattaque, puisque c’est un travail malheureusement continu. Précisément, comment peut-on assurer, en cas de cyberattaque, une continuité de service ? Il y a cette notion de doublon humain auquel, au sein de notre groupe, on est particulièrement attentif : s’il y a une solution informatique, il devrait toujours y avoir aussi une personne de contact, un numéro de téléphone où ce n’est pas une machine qui répond, mais un contact humain. Cette possibilité existe-t-elle toujours, si jamais les ordinateurs sont en panne ? C’est bien beau d’avoir quelqu’un de l’autre côté, mais y a-t-il cette notion de présence humaine, sachant aussi qu’il peut y avoir chez nombre de nos concitoyens une fracture numérique ? Comment associer à la fois la lutte contre la fracture numérique et la présence humaine en cas de cyberattaque ?

J'en viens à une deuxième notion : la protection des données, puisque nos concitoyens peuvent envoyer sur les différents services du SPW ou officiels des données sensibles, personnelles, voire financières et de santé. Comment s'assurer qu'elles puissent être, au mieux, immunisées contre des fuites de données dans le cadre d'une cyberattaque ? Si, par impossible, il devait y avoir des fuites constatées, existe-t-il une procédure prévue pour informer les citoyens que des données personnelles auraient pu partir et auraient pu être captées par des personnes pas nécessairement bienveillantes et utilisées ? Existe-t-il des outils particuliers pour protéger ? Existe-t-il des procédures en cas de fuite, notamment pour informer les citoyens concernés ?

Vous êtes plusieurs aujourd'hui, donc cela signifie que plusieurs services sont concernés. Certains de mes collègues ont déjà évoqué la notion de coopération. Comment s'assurer qu'il y ait des modalités de coopération entre les différentes unités, sachant que chacune a ses propres modalités, sa propre culture d'entreprise et donc ses propres logiciels qui ne sont pas nécessairement les mêmes ? Quelles sont les modalités de coopération ?

Quatrième sujet, c'est par rapport aux ressources humaines. Cette notion de cybersécurité est de plus en plus prégnante. Quel accompagnement est prévu pour les différents agents ? Y a-t-il une formation systématique continue de la part des personnes directement en charge de cette thématique, mais aussi tout un chacun ? Ils peuvent être tous, à leur insu, vecteurs d'une cyberattaque. Y a-t-il une sensibilisation particulière ? Y a-t-il non seulement des réflexes, mais des procédures à déterminer, dès lors qu'il y a une suspicion de cyberattaque ou de pratiques peu sécurisées qui seraient constatées ?

Un autre élément, toujours en lien avec les agences, est : quid par rapport à l'intelligence artificielle ? Quelle est cette politique ? On injecte plus de notions de sécurité pour se prémunir, et, en même temps, on donne les éléments pour être plus facilement attaqués. Quelle politique est établie par rapport à l'intelligence artificielle ?

Toujours en termes de ressources humaines, en ce qui concerne la politique au sein du SPW relativement à la formation des personnes, la roue du temps fait son œuvre. Ces personnes, à un moment donné, soit partent à la pension bien légitimement, soit décident de changer d'emploi pour des raisons qui leur sont propres. Une politique est-elle menée pour s'assurer de conserver les différentes compétences qui y sont développées ?

Il y a le lien sur la question des moyens et des besoins. Sont-ils en adéquation les uns par rapport aux autres, sachant que l'on ne sait jamais l'étendue et l'immensité des possibilités des cyberattaques ? On ne peut pas couvrir toutes les hypothèses. On serait déjà bien en peine de les nommer. Néanmoins, il convient

d'avoir quelque chose considéré raisonnablement comme une politique robuste par rapport à ce qui nous occupe.

D'un point de vue pratique, les serveurs sont-ils des serveurs physiques ou sont-ils à l'extérieur ? Si oui, des notions de back-up sont-elles prévues ? On a vu que des serveurs extérieurs hébergés pouvaient être soumis à des incendies, même pas dans le cadre d'une attaque terroriste, mais purement physiquement.

En termes toujours de moyens, sachant le nombre d'ordinateurs qui équipent la fonction publique, le hardware est-il adapté ? Le software l'est-il également ? Quelle politique est menée en fonction de cette notion de cyberattaque ?

Je ne suis pas plus long à ce stade. Je laisse le soin à mes collègues de développer d'autres éléments, mais je ne voudrais pas que mes questions soient plus longues que les présentations.

Mme la Présidente. – La parole est à Mme Cremasco.

Mme Veronica Cremasco (Ecolo). – Bonjour à tous et à toutes, merci beaucoup d'être là et d'être venus nous éclairer sur cette cyberattaque. Je voudrais avoir un petit à petit message pour les équipes du SPW en particulier. Quelle que soit la catastrophe – des inondations, des canicules ou une cyberattaque –, on sait à quel point tous les employés du SPW sont sur le front, sont eux-mêmes, presque dans leur vie privée, directement concernés par la gestion de la crise. On l'oublie un peu parfois, et c'est important de les remercier et de leur dire que l'on est avec eux. Si vous pouvez transmettre mon message, ce serait gentil. Merci à vous d'être avec nous.

J'ai bougé toute une série de questions pour ne pas être redondante, notamment par rapport à la gestion de la crise en tant que telle. Mme Tillieux notamment, a été assez exhaustive, elle a été complétée par quelques collègues. Je vais essayer de ne pas redire des choses qui ont déjà été dites.

Des collègues ont déjà posé la question concernant le renforcement des équipes, l'aspect des ressources humaines de l'après-crise. J'aimerais poser la question à Mme Roucou et à Mme la Ministre : de combien de personnes était composé le pôle sécurité avant et de combien de personnes est-il composé maintenant ? Quel est le statut de ce personnel ?

De plus, j'ai une question liée à la souveraineté numérique et d'autres questions qui ont été posées par les collègues. Combien de consultants externes ou internes renforcent aujourd'hui ce pôle de sécurité ? Comment fait-on en prenant la dimension sécurité ? C'est pour cela que je faisais allusion à la souveraineté numérique, en demandant s'il s'agissait d'internes ou d'externes. Cela a-t-il un poids sur la sécurité ? Quelle

est l'évolution des budgets qui sont alloués aux consultants externes ? Madame la Ministre et Madame Roucou, si vous avez toutes les deux la même réponse, cela m'arrange. Comment les budgets alloués aux consultants externes ont-ils plus précisément évolué par rapport aux trois dernières années ?

Par ailleurs, vous avez tous parlé des faiblesses et des défauts qui ont été identifiés par rapport au système. On en a identifié une partie pendant la crise, il y a eu quatre groupes d'interlocuteurs. Des audits sont-ils encore réalisés aujourd'hui ? Si oui, comment ? J'ai toujours la même préoccupation : avec des internes ou des externes ? Fait-on des audits couramment ? À quelle fréquence ?

Pour ma part, je suis souvent soumise à ce que l'on appelle des *penetration tests*, que ce soit dans le cadre du Parlement ou dans le cadre de fonctions précédentes. On fait des simulations d'intrusion. Ce type de simulation est-il fait sur nos services ? Si oui, quelles en sont les conclusions ? N'hésitez pas à me dire que c'est complètement obsolète, que tout le monde a bien compris que cela ne marche pas, et cetera. Pour y être moi-même confrontée, pas au quotidien, mais quasiment, je me demande si cela fonctionne.

On a beaucoup mis en évidence le côté obsolète des infrastructures, notamment des systèmes d'exploitation. Nous savons tous, même les plus béotiens d'entre nous, qu'un système d'exploitation nécessite d'être mis à jour, aussi en matière de sécurité. Nous y sommes aussi confrontés au quotidien. Y a-t-il encore des systèmes d'exploitation qui sont aujourd'hui jugés obsolètes au SPW ? Si oui, combien ? Quelle est la feuille de route ? Je ne vous demande pas de me livrer des détails qui nous mettraient en péril, même si je ne crois pas que ce soit une information « secret de la Défense ». Où est l'état du parc ? A-t-on supprimé ces serveurs qui seraient obsolètes ou qui ne seraient pas mis à jour ? Quelle est la feuille de route les concernant ?

On a aussi beaucoup parlé des difficultés du système. Vous les avez énoncées en disant qu'il y avait quatre points, notamment dans un des deux exposés. Je crois que Mme Roucou a bien mis en évidence les difficultés du système. Par contre, vous avez moins parlé, me semble-t-il, de la gestion du risque à proprement parler. J'ai commencé mon intervention en abordant les inondations, les feux de forêt, et cetera. Je m'adresse aussi à M. Guisse. La gestion du risque, c'est une des priorités en Wallonie par rapport au SPW, mais, en général, gérer le risque, c'est une priorité transversale, me semble-t-il.

Par rapport à cette gestion du risque, au niveau de votre socle informatique, en termes de probabilité, en termes d'impact, avez-vous identifié comment on gère le risque par rapport à cela ? Avez-vous un tableau des risques ? Quelle est sa fréquence de mise à jour ? Quelles mesures ont été prises pour mitiger ce risque ?

Pouvez-vous donner des exemples concrets de modifications, notamment par rapport au socle informatique depuis 2025, pour mitiger ces risques ?

Concernant l'avis de vulnérabilité, j'ai compris que le service fédéral avait été mis au courant et que vous aviez tous été mis au courant en cascade. Par rapport à ces avis de vulnérabilité lors d'attaque en direct – où l'on vous dit que l'on est vulnérable et qu'il se passe quelque chose pour les composants de la solution informatique –, comment fonctionnent ces avis de vulnérabilité et quelles sont les mesures qui seraient éventuellement prises pour les réduire ? Ce qui a fort marqué notre assemblée et la population, c'est le temps de réaction. Si l'on est vulnérable sur un point, combien de temps cela prend-il pour le mettre à jour ? Comment cela fonctionne-t-il ?

Le Service fédéral des polices a indiqué qu'il ne savait pas identifier globalement l'entreprise du SPW, parce qu'elle n'est pas assez structurée. Vous avez même dit, sauf si je me trompe, que cela fonctionnait par silo et que c'était un peu compliqué à appréhender. Au niveau de l'architecture même de l'entreprise du SPW, des décisions ont-elles été prises ?

Vous avez dit que vous alliez ajuster votre stratégie métier à la stratégie des systèmes informatiques. Où en êtes-vous ? Au niveau du Fédéral et de la Computer Crime Unit, leur donnez-vous des informations pour leur dire que cela semble plus gérable dans la restructuration globale de toute l'architecture, en fonction des métiers qui sont exercés dans le SPW ? Je me doute que vous avez des consignes de sécurité pour la restructuration de toute l'entreprise SPW. C'est important que les services de police fédéraux soient au courant de cette architecture d'entreprise et aient leur avis sur le sujet.

Au niveau de la sécurité, on me fait tout le temps changer de VPN au Parlement wallon et d'autres choses. J'imagine que vous travaillez sur la problématique des gens qui travaillent au SPW qui sont connectés via l'extérieur. C'est comme nous : on est connecté au Parlement, mais il faut activer les VPN, les mots de passe, les utilisateurs, et cetera. Comment cela fonctionne-t-il ? Est-ce un sujet d'inquiétude ? À quelle vitesse renforcez-vous ces sécurités par rapport aux agents : les VPN, les rotations des mots de passe, et cetera ? Est-ce un point de fragilité ? J'imagine que oui, parce que ça l'est dans toutes les entreprises. Est-ce qu'on y fait face ? Sauf erreur, je n'en ai pas entendu trop parler et cela m'étonne un peu, parce que j'ai l'impression que c'est un point faible de tous les systèmes et toutes les architectures informatiques.

J'ai une dernière question très pratique. Je m'occupe beaucoup d'aménagement du territoire, et cetera. Il y a là-dedans beaucoup d'enquêtes publiques, beaucoup de documents qui nécessitent une information suffisante, correcte, mise à jour. Quand la cyberattaque est arrivée,

cela a été complexe par rapport à cela, mais je ne fais pas de jugement. On pourrait aller plus vite. Je l'espère, sans quoi on ne serait pas ici. Par rapport aux démarches et aux procédures, il y a pas mal de droits et d'obligations légales qui sont derrière ces informations. Quelles sont vos réflexions par rapport au rétablissement du service en tant que tel ? Cela rend, en effet, des tas de procédures légales caduques.

Quelles actions sont entreprises pour que cela soit préservé, pour qu'il y ait au moins une transmission d'informations auxquelles on sait que l'on ne touche pas ? Par exemple, pour un permis de bâtir, une cyberattaque pourrait provoquer un délai de deux jours, mais on pourrait faire en sorte que ces données soient directement récupérables et que ces démarches et procédures puissent continuer. Quelque chose est-il mis en place pour que cela soit effectivement le cas ?

Mme la Présidente. – Tous les groupes se sont exprimés. Je propose donc de rendre la parole aux intervenants, chacun à leur tour, pour répondre aux questions.

La parole est à M. Guisse.

M. Stéphane Guisse, Secrétaire général a.i. du Service public de Wallonie (SPW). – On est un peu en *assessment*.

(Rires)

Je vais d'abord répondre aux questions de Mme la Députée Tillieux.

Comme je l'ai dit, à l'époque de la cyberattaque, je n'étais pas à la manœuvre, mais je n'étais pas loin. Je peux donc déjà répondre à une question posée par plusieurs d'entre vous : qui dirigeait le SPW Digital ? C'était Sylvie Marique, qui était alors secrétaire générale et qui a repris la main au départ de la DG du digital, puisque le digital était, déjà à l'époque, une entité du Secrétariat général. Mme Marique avait donc l'autorité hiérarchique sur le digital et sur le support. Je tiens à souligner que, à l'époque, elle n'avait plus non plus de DG du support et qu'elle assumait donc l'entière responsabilité de la gouvernance du périmètre du Secrétariat général.

Dès que la crise a été identifiée, comme l'a dit ma collègue Isabelle Quoilin – c'est-à-dire dès le mardi 15 avril, lorsque les premiers signaux d'alerte ont été partagés entre les membres du Comité stratégique, ce qui m'a fait découvrir l'imminence de la menace –, nous avons été associés.

Par rapport au dossier de reprise-remise, j'ai eu la chance de suivre de très près les travaux. Je n'avais pas tous les détails, notamment les détails confidentiels concernant l'enquête judiciaire, mais j'ai pu, avec mes collègues du Costra de l'époque, suivre de très près la stratégie de contingentement du risque, de

débranchement et de remise en route régulière des actifs. Cela m'a permis, le jour où j'ai pris mes fonctions de manière assez brutale, le 23 juin, d'avoir derrière moi toute cette connaissance accumulée au fil des semaines en tant que DG des finances. Je ne partais donc pas de zéro. Évidemment, quand je suis arrivé, le premier mois a été extrêmement intensif. Les collègues du SPW Digital – notamment Mme Quoilin – m'ont briefé en me transmettant toute une série d'informations. J'avais aussi la chance que le premier rapport d'incident était en voie de finalisation. J'ai donc pu assister à la publication du rapport qui a été remis, notamment, au Parlement wallon, et je suis allé chercher les infos qu'il me manquait en tant que directeur général.

Par rapport à cette expérience, je me veux un peu rassurant. Je vais répondre en bloc à quelques questions. Quand on fait le bilan, avec l'année et demie de recul, je pense que les conséquences pour les citoyens et les entreprises de Wallonie ont heureusement été limitées dans le temps. Par exemple, les paiements constituaient un grand bloc qui était prioritaire pour le SPW Finances. En effet, le SPW assume quotidiennement, en moyenne, 350 à 500 paiements de factures commerciales et quasiment le double de subventions et de primes. Il était donc impératif que nous puissions récupérer au plus vite notre force de frappe comptable. Ce fut le cas : la plateforme WBFIn SAP, qui permet les liquidations, a été le premier système rouvert, après environ 48 heures. Nous avons trouvé – c'est un autre sujet qui a été évoqué – des solutions tactiques de contournement permettant de contrer l'absence du web. Notre banquier, qui était Belfius et qui l'est toujours, nous a aidés, en quelques jours, à remonter quelque chose. On est donc restés, en tout et pour tout, quatre ou cinq jours calendrier sans pouvoir payer. C'était une priorité absolue pour le monde économique et pour les citoyens que de pouvoir honorer les paiements qui étaient dus.

Un deuxième grand bloc, c'est le bloc fiscal. Je ne vous étonnerai pas en vous disant que les citoyens étaient plutôt contents de notre incapacité à taxer. Nous n'avons connu aucune conséquence pour le précompte immobilier. J'ai eu très peur à l'époque, mais nous avons pu restaurer le système dans les temps pour ne pas compromettre la campagne 2025 de taxation du précompte. En matière de véhicules, nous taxons mensuellement. Cela signifie que, tous les mois, on sort à peu près 200 000 à 250 000 documents fiscaux. Là, on a eu quasiment deux campagnes de retard, soit jusqu'à deux mois de retard pour envoyer les documents. Cela veut dire que l'on a envoyé, en une seule fois, 600 000 à 700 000 documents. Le retard en fiscalité s'élevait donc à deux mois de décalage ; on a évidemment adapté les délais de paiement à due concurrence. On a été extrêmement souples, à l'époque, par rapport au recouvrement : on l'a suspendu et l'on a allongé les délais de paiement pour ne pas préjudicier les citoyens et les entreprises.

Madame Cremasco, vous parliez des permis. Effectivement, c'est un autre volet qui a été fort impacté. À cet égard, le Gouvernement a pris les mesures qui s'imposaient pour prolonger tous les délais de rigueur pour faire face à la crise. De mémoire, c'était de deux à trois mois. A priori, avec le recul, aucun citoyen n'a été lésé sur le long terme.

Évidemment, on a eu un impact pendant cette période de cyberattaque, approximativement entre le mois d'avril et le mois de juillet, mais, une fois passé le mois de juillet, on a récupéré un certain fil de l'eau par rapport aux démarches. Je peux vous dire aujourd'hui que, normalement, il n'y a pas de préjudice grave.

Je laisserai mes deux collègues présenter l'inventaire de ce qui est fait et de ce qu'il reste à faire.

Pour répondre à Mme Tillieux, il y a trois décisions à prendre. La première est vraiment importante. Cela n'a pas été un scoop pour moi, puisque, à propos de l'histoire du SPW, je fais partie des « dinosaures » maintenant. Cela fait 30 ans que je suis dans la fonction publique wallonne. J'ai connu le MET, j'ai connu la création du SPW, j'ai vu les évolutions successives du SPW. C'est mon troisième COSTRA. Le SPW s'est un peu construit à partir de bric et de broc : on a des morceaux d'administrations qui venaient de différents endroits, on a des UAP qui ont été intégrées. Il est indéniable que, si l'on revient un an et demi en arrière, nous avons effectivement des solutions informatiques qui venaient d'horizons différents. Je ne conteste pas du tout le côté hétéroclite du parc applicatif. Quand on prend le rapport qui a été établi en juillet 2025, nous parlions de 800 applicatifs différents au SPW : certains applicatifs majeurs qui concernaient des milliers de personnes, quelques applicatifs légers qui concernaient les 10 à 15 utilisateurs.

Une des premières opérations dans le Plan de relance est de décommissionner les applicatifs trop obsolètes et trop dangereux, de faire un grand pas en avant dans la mise en place d'outils plus modernes. On a donc mutualisé ce que l'on pouvait. Il est clair que l'on ne passe pas de 800 applicatifs à 15 ou 20 applicatifs en quelques mois. Nous avons donc encore aujourd'hui des centaines d'applicatifs qui tournent au SPW, mais nous avons une trajectoire tout à fait réaliste et tenable de réduction progressive du parc pour aller vers un parc plus serein.

Voilà pour ma première décision, qui est de dire stop aux produits beaucoup trop obsolètes et de privilégier les solutions pérennes de grande masse du style SAP, du style Odoo, entre autres. La suite Microsoft, qui est déployée depuis quelques années, a été pour moi un facteur de relative sécurité de nos sites informatiques.

La deuxième décision est une gouvernance beaucoup plus centralisée, que Sylvie Marique avait commencée. On reprend le flambeau avec ma collègue,

Isabelle Roucou. L'informatique, aujourd'hui, ne peut plus se décider dans des comités de direction isolés, dans des départements du SPW ; il faut impérativement un pilotage d'ensemble. J'estime que, depuis ces 15 derniers mois, ce pilotage d'ensemble est assuré. Nous avons des débats très réguliers avec des collègues directeurs généraux.

Je réponds ici à une autre question : tous les mois, nous avons un point de comité stratégique dédié à la sécurité. C'est Mme Quoilin, ici présente, qui vient passer une heure avec nous afin de faire le point, de présenter l'état d'avancement des plans de restauration, de comment on s'améliore, de ce qu'il reste à faire. L'inventaire des besoins est extrêmement précieux, c'est un moment de grande écoute. Tous les PC sont fermés, on s'écoute mutuellement et l'on construit ensemble ce plan de résilience et de restauration du SPW.

La troisième décision à prendre – ce sujet a été beaucoup évoqué par chacun des partis – est de trouver le bon mix entre travailleurs publics et travailleurs privés. Pour ceux qui me connaissent, je suis un grand défenseur de l'emploi public, c'est-à-dire de l'internalisation de compétences, mais l'IT est vraiment un secteur pour lequel il est extrêmement compliqué d'internaliser.

Depuis quelques années, j'ai connu toute une série de tentatives successives d'internaliser des postes. Nous avons reçu de la part des gouvernements successifs des enveloppes particulières pour créer des postes en interne. Que cela est compliqué ! Quand on reçoit quelques dizaines de cartouches RH à consommer, même avec des barèmes relativement intéressants – ce sont des postes experts, parfois A5 ou A4 –, on est resté parfois deux à trois ans sans trouver ne fût-ce qu'un candidat sur un poste. Nous étions condamnés, malgré cette cartouche qui nous était offerte, à prendre des prestataires privés.

Nous avons des échelles de paiement qui varient très fort. Les grands profils « experts » se payent à des prix que nous ne pourrions jamais assumer en termes d'emploi dans la fonction publique. L'IT, et l'IA en particulier, est un secteur où nous devons malheureusement vivre avec une certaine mixité entre public et privé. Notre grand défi, à tous les trois ainsi qu'à tous les collègues qui ne sont pas ici avec nous, est de trouver ce bon mix. Quelles sont les fonctions à internaliser, quelles sont les fonctions à sous-traiter à l'extérieur ? Nous avons essayé dans les grands pôles de sécurité, dans le « régalién numérique », d'avoir des ressources en interne. Je ne joue pas à Calimero. En 15 mois, j'ai appris à mieux connaître les collègues du SPW Digital et du SPW Secrétariat général. Nous pouvons compter sur une somme de compétences et de talents inimaginable et je pense que c'est ce qui nous a vraiment sauvés il y a un an et demi, pour limiter la casse. Nous pouvons compter sur des fonctionnaires qui sont là et gardent la boutique. Nous avons aussi des

partenariats avec des firmes privées de grande qualité qui viennent compléter les compétences. Nous sommes vraiment dans une synergie entre public et privé sur l'aspect digital.

Monsieur Massaki Mbaki, vous avez cité l'importance du facteur humain, et vous avez mille fois raison. En effet, on l'a dit dans notre intervention, le meilleur système du monde n'est rien si l'on n'aide pas nos collaborateurs à être formés à une bonne utilisation. Mme Cremasco a parlé de sensibilisation, c'est clair que cette dernière est très présente. Nous avons des modules de formation obligatoire pour tous les agents du SPW. Nous avons des tests d'intrusion réguliers avec des bilans personnalisés. Nous n'avons encore fustigé personne, mais il est clair que la personne qui, tous les mois, se fait choper pour la quatrième ou cinquième fois, on commence à lui remonter les bretelles pour lui dire : « Soyez un peu prudent ».

Mme Veronica Cremasco (Ecolo). – On va vous engager pour travailler ici ! Les pauvres !

(Rires)

M. Stéphane Guisse, Secrétaire général a.i. du Service public de Wallonie (SPW). – Je suis quelqu'un d'assez bienveillant en général. C'est évidemment vital puisque les failles de sécurité, c'est souvent par ce canal que cela survient. C'est quelqu'un qui branche une clé USB venant de l'extérieur, c'est une connexion pas sécurisée, c'est un PC qu'on laisse ouvert sans mise en veille dans un lieu public. Ce sont vraiment des petites choses sur lesquelles on apprend de manière systématique et régulière à nos collaborateurs, soit à être extrêmement prudents. À propos du facteur humain, je suis tout à fait d'accord.

Je laisserai la question de l'IA à mes deux collègues, puisque c'est un facteur évidemment tout à fait clé.

Monsieur Liradelfo, j'ai un peu répondu à la question : les retards imputés à la crise ont été limités dans le temps. Je pense honnêtement, un an et demi après, qu'il n'y a pas de conséquences définitives, graves ou très dommageables pour les usagers. On a eu cette période de vide pendant quelques semaines où plein de services étaient coupés, et c'est vraiment là que l'on a mesuré parfois tout ce que l'on peut apporter comme services publics, comme biens publics à la population. C'est quand on coupe toute une série de services que des gens consommaient sans même savoir qu'on était derrière, que l'on s'aperçoit de la plus-value que peut apporter un service public à la vie au quotidien.

Je pense que toutes les autres questions vont relever plutôt des spécialistes en informatique dont je ne fais pas partie.

Mme la Présidente. – La parole est à Mme Roucou.

Mme Isabelle Roucou, Directrice générale du Service public de Wallonie Digital (SPW Digital). – À propos du SOC qui existe depuis juin 2025, nous étions en effet occupés à préparer ce dossier d'achat d'un SOC depuis un certain temps via un marché public avec les collègues de l'équipe de cybersécurité. Dès lors, le SOC était bien dans nos priorités. Crise ou pas crise, le SOC serait arrivé et aurait été installé dans les mois qui venaient.

Avec la crise, on a pris l'option d'un SOC d'urgence. Entre-temps, nous l'avons remplacé à l'échéance du marché public par un autre SOC qui nous permettra d'avancer dans les prochaines années et de renforcer chaque mois, chaque semaine, davantage nos protections vers une plus grande résilience et un plus grand périmètre de couverture.

Concernant les moyens humains et les compétences disponibles, M. Guisse a mentionné les nombreuses compétences existantes au SPW, non seulement dans l'équipe de cybersécurité interne et externe, mais également dans tous les services du SPW Digital et d'ailleurs.

Vous parliez de dépendance technique et du fait qu'elles soient ou non testées. Nous testons régulièrement une série de dépendances. Les testons-nous toutes ? Peut-on dire un jour que l'on teste toutes les dépendances ? C'est vraiment difficile, mais nous en testons quelques-unes avant ; nous en testons définitivement beaucoup plus maintenant, et chaque jour davantage.

Vous avez parlé du fait que j'étais inspectrice générale. Je n'étais pas inspectrice générale, j'effectuais une mission de consultance, d'accompagnement de l'équipe exploitation. Je n'avais pas du tout les attributs ou les possibilités de décision qu'un inspecteur général a. J'accompagnais une équipe. N'ayant pas d'inspecteur général dans cette équipe, David Wattecamp avait les deux rôles : le directeur général prenait le rôle d'inspecteur général également. Je le conseillais et j'accompagnais les équipes. C'est important de le préciser.

Je suis ravie de vous entendre dire que le SPW Digital souhaitait ma prolongation comme consultante à l'époque, cela fait plaisir à entendre. Je suis ravie d'être venue dans un rôle de fonctionnaire contractuel, parce que c'est une belle maison.

Vous avez parlé d'obsolescence. Il y a énormément d'applications qui datent de longtemps. Chaque mois, chaque trimestre, chaque semaine, nous améliorons la maturité technologique de nos applications, en les remplaçant par de grands socles technologiques, par de grandes plateformes. Nous essayons de faire déplacer des applications plus anciennes vers ces grandes plateformes sur lesquelles nous travaillons.

Cela vient de la FCCU. Mme Derkoningen mentionnait qu'elle avait constaté de nombreuses décentralisations et de décentralisations des décisions. Toutes ces applications – qui étaient diverses et variées, gérées dans les métiers – ont constitué l'obsolescence, parce que la priorité était souvent donnée à l'amélioration et à l'augmentation de fonctionnalités plutôt qu'à la correction et à la mise à niveau des logiciels et des matériels.

J'ai pu constater, depuis mon retour – c'est certainement un des bénéfices de la crise –, qu'une attention beaucoup plus grande est donnée au respect et à l'amélioration de ces socles technologiques ainsi qu'à la prise en compte du SPW Digital et de la cybersécurité.

Vous me demandiez trois décisions à prendre pour éviter que la crise ne se produise. Nous avons un magnifique outil, qui s'appelle NIS 2, avec un grand nombre de mesures. Encore mieux, il y a un outil créé par la Belgique au CCB, CyFun, qui l'a bien structuré. Cela doit être notre feuille de route des prochaines années. Sur les différents piliers que je vous ai présentés, le CyFun aide tous les départements IT et tous les départements métiers à se structurer, de la gouvernance jusqu'à la détection et la récupération des applications et des systèmes pour les métiers.

Une décision serait d'aller à fond là-dedans et sur tous les piliers de NIS 2 en parallèle. Des personnes différentes peuvent y travailler. Il y en a pour des gens techniques dont je vous ai parlé régulièrement dans mon discours. De plus, la sécurité n'est pas qu'une affaire de spécialistes. Elle est aussi une affaire de management, de *change management*, de changement de culture, de gouvernance, de mise en place de processus structurés. La sécurité en 2026, c'est un ensemble de compétences humaines, organisationnelles et techniques qui se mettent ensemble au service d'une organisation. La première chose que je dirais, c'est d'aller à fond dans ce système et de travailler sur l'ensemble des recommandations.

Mon souhait est également de moderniser le plus possible les applications et, si on ne peut pas les moderniser, de les « buller » – pour utiliser un grand mot auquel on a eu recours pendant la crise – ou de les mettre dans une forteresse pour que l'on puisse continuer à les utiliser sans risque. J'ai un autre souhait : que les métiers travaillent ensemble avec nous pour soit moderniser une application, soit décider de ne plus l'utiliser si elle n'est utile que pour un faible nombre de gens ou aller vers les grandes plateformes transversales proposées par le SPW Digital – M. Guisse en a cité quelques-unes. C'est important d'aller dans cette direction, aussi bien dans un environnement Microsoft, SAP ou Odoo, qui va gérer les subventions, et cetera.

Le troisième point, comme M. Guisse l'a indiqué, c'est qu'il est extrêmement difficile, en 2026, d'aller

seulement vers des travailleurs du public. Il importe de renforcer la collaboration entre les travailleurs publics et les consultants externes qui sont avec nous, de trouver d'autres manières astucieuses de convaincre les travailleurs venant du privé de venir nous rejoindre. Ce n'est pas si facile, en effet : certaines fonctions étaient ouvertes depuis près de deux ans en cybersécurité sans que personne n'ait postulé. Dans ce cas, il vaut mieux qu'un consultant externe occupe la place, plutôt que personne. Ce sont mes trois souhaits.

Monsieur Massaki Mbaki a demandé quels indicateurs permettraient de voir les avancées du SPW en matière de cybersécurité. J'ai parlé de NIS 2. Pour moi, NIS 2 permet, tout en donnant une série d'indicateurs d'amélioration et des propositions, de mesurer la maturité actuelle. Une mesure de la progression, ce sera de le mesurer de manière régulière. D'ailleurs, on doit atteindre un certain score pour une certaine date, le mesurer et voir comment on s'améliore par rapport à cela. Des indicateurs existent : on ne doit donc pas inventer beaucoup de choses.

Les formations sont également importantes. Vous demandiez comment s'assurer que les gens continuent à se former. Nos techniciens se forment pour les plateformes qu'ils doivent gérer. Nous sommes très attentifs à cela. Mais ils se forment aussi en matière de cybersécurité. De nombreuses formations vont être proposées, par exemple, à tous les managers du SPW, en partenariat avec l'EAP. C'est important. On reviendra plus tard, peut-être sur les questions concernant l'IA.

On teste aussi de nombreuses choses à l'heure actuelle. Il ne s'agit peut-être pas encore de tests complets, mais, par rapport à il y a deux ans, de nombreux tests réalisés à des endroits spécifiques nous permettent d'améliorer notre posture de sécurité. On teste les *back-ups*, l'arrêt système et le redémarrage, on teste des choses au niveau du réseau. On a mis en place une série de choses qui nous permettent d'améliorer notre résilience. Nous avons encore un grand chemin à parcourir – nous ne l'avons pas caché –, mais chaque jour nous en rapproche.

Nous avons également réalisé énormément de recommandations parmi la liste fournie par Microsoft, CCB, et cetera. Si elles n'ont pas encore été réalisées, pour certaines, c'est parce que nous les avons mises dans le programme cybersécurité géré par ma collègue Quoilin et c'est probablement trop lourd pour un yaka. Nous le prévoyons en projet et en sous-projet dans les prochaines semaines, les prochains mois, voire les prochaines années.

Certaines personnes ont parlé de serveurs physiques, d'acteurs. Y a-t-il des *back-ups* ? Oui, nous faisons des *back-ups* de nos systèmes. Nous avons toute une série de choses qui sont mises en place.

Une personne parmi vous a posé une question quant au danger induit par le fait de ne pas laisser les métiers gérer une diversité de systèmes. Non, il vaut mieux que ce soit un minimum standardisé par l'IT. Si des métiers souhaitent utiliser un système particulier, il est mieux de l'analyser, de l'intégrer dans notre système d'information, dans nos standards, et de réduire le nombre de standards. On n'a jamais à gagner à avoir une trop grande diversité de systèmes. Par contre, on pratique le *dual vendor*, avec au moins deux systèmes, qui nous permet d'éviter de mettre tous nos œufs dans les mêmes paniers. À côté, par exemple, de Microsoft, nous avons toute une série de choses qui nous offrent d'autres possibilités de réagir.

Procédons-nous à des *penetration tests* ? Oui, nous en faisons sur base régulière. J'aimerais même en faire encore plus. Peut-être que l'IA pourra nous aider à développer cela pour nous permettre de les faire encore plus vite dans le futur.

Mme la Présidente. – La parole est à Mme Quoilin.

Mme Isabelle Quoilin, Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital). – Je vais essayer de m'y retrouver entre ce qui a déjà été répondu et ce qui n'a pas encore été répondu.

Je reviens deux minutes – puisqu'on me l'a redemandé – sur mon rôle pendant la crise. À ce moment-là, j'étais conseillère en stratégie auprès du directeur général du SPW Digital. Comme vous le savez, il n'y avait plus de directeur général. Dans le cadre de mes missions, j'étais en charge d'accompagner le pôle sécurité pour le faire grandir en maturité et intégrer cela dans la réflexion totale du SPW Digital. C'est ainsi que la secrétaire générale m'a demandé de la seconder pour cette partie de coordination dans la gestion de la crise. Ce n'était pas ma responsabilité hiérarchique, mais c'est effectivement un rôle qui, du fait de mes anciennes fonctions – comme Mme Tillieux l'a rappelé –, était dans mes compétences et me permettait d'apporter mon soutien à cet égard.

Des questions ont été posées sur la situation à ce moment-là. On l'a dit, en toute modestie, notre sécurité avant la crise n'était pas très élevée au SPW. C'était quelque chose qui était connu, mais qui n'était pas nécessairement pris en compte et intégré suffisamment dans les plans d'action. C'est une des conséquences positives de la crise : elle a remis à sa bonne place la question de la cybersécurité dans les priorités, aussi bien de l'administration que du Gouvernement.

Toute une série d'éléments manquaient dans la gestion de la crise. Ceux-ci ont globalement été – je dois le signaler – compensés par l'expertise et l'expérience du personnel de l'administration, que ce soit au niveau IT ou au niveau métiers. Ceux-ci, par leur expérience, leur compétence et leur expertise, ont pu finalement assumer la gestion de cette crise en minimisant les

impacts. Comme je l'ai dit, il y a eu effectivement des impacts sur la disponibilité des systèmes pendant un certain temps, mais globalement, il n'y a pas eu, comme M. Guisse l'a rappelé, ni destruction ni vol massif de données, et probablement même pas de vol de données du tout. Par rapport à toutes ces questions sur la situation avant la crise, c'est vraiment le message que je voudrais faire passer. Depuis lors, nous avons énormément évolué.

On a beaucoup posé la question des budgets. En 2025, le Gouvernement nous a accordé un budget complémentaire suite à la crise, qui s'est élevé en crédits d'engagement de 8 millions pour le SPW Digital et de 2 millions pour le SPW Mobilité et Infrastructure. Ce sont les fameux 10 millions dont on a beaucoup parlé l'année passée. Ces montants ont servi, pour une petite partie, à payer les conséquences directes de la crise, comme l'accompagnement de Microsoft DART qui nous a accompagnés pendant cette crise.

Ces montants nous ont principalement servis à financer de manière accélérée des projets ou mesures qui étaient dans les cartons. On a parlé tout à l'heure du SOC qui était dans nos travaux en cours et qui voyait une échéance à plutôt moyen ou long terme. Cela a accéléré toute une série de projets de résorption d'obsolescence, de mise en place d'outils et de technologies dont nous avions besoin, qui n'étaient pas considérés comme prioritaires avant cette crise et qui le sont devenus. Cela a transformé la dynamique à tous les niveaux. Je tiens à le souligner, parce que cela a été très positif et cela perdure ; même si l'on a craint qu'une crise en chasse une autre, on ressent bien que l'on a un soutien qui perdure en la matière. C'était un message assez positif.

On a beaucoup parlé du SOC, je vous apporte quelques précisions le concernant. Pendant la crise, on a mis en place un SOC d'urgence. On avait presque un cahier de charges fini au moment où la crise est arrivée. On a sorti une version raccourcie de nos exigences SOC pour faire ce SOC d'urgence pendant la crise. Pendant la période où l'on était couverts avec ce dernier, on a finalisé nos prescriptions techniques détaillées et pu lancer, fin de l'année passée, un marché qui a été attribué au mois de mai. Ce SOC actuel, qui est prévu pour une durée de quatre ans plus deux plus deux, selon le marché public, a une vocation à être beaucoup plus étendu, avec des fonctionnalités plus larges et un périmètre plus large. On est dans cette phase progressive d'extension de la couverture et des fonctionnalités de ce marché SOC qui, probablement, va durer jusqu'au milieu ou la fin de l'année prochaine pour atteindre son niveau de maturité maximale, comme prévu par le cahier de charges. C'est le planning tel que prévu par le marché sur lequel on est en train de travailler.

Je ne vais pas revenir sur les besoins RH, puisque cela a déjà été beaucoup abordé, si ce n'est qu'après la crise, les équipes sécurité ont été renforcées, ou en tout

cas stabilisées pour une partie, avec toutes ces questions internes et externes qui restent complexes. J'ajouterais que ce n'est pas qu'une question de salaire : aller chercher des personnes à temps plein au sein de l'administration dans des fonctions si volatiles et avec une pression sur le marché aussi importante que celle qui concerne tous les experts cyber, c'est très compliqué. Parfois, même pour un salaire inférieur avec des externes, on arrive à les capter parce qu'ils restent libres de partir quand ils veulent ou quand ils ont un meilleur contrat qui les attend ailleurs. On doit tenir compte aussi de cette réalité du marché de l'emploi de la cybersécurité.

Je reviens sur le budget. On a eu un budget complémentaire l'année passée suite à la crise et l'on peut constater que cette année, nous avons eu un budget équivalent sur le budget sécurité au niveau du SPW Digital. Si l'on est dans la continuité et que l'on maintient ce niveau assez élevé, néanmoins suffisant en termes de capacité de l'administration à absorber ce budget et cette importance, notre demande est de rester à ce niveau de manière pérenne. Effectivement, cela demande un effort de la part du Gouvernement et on espère que ce message perdurera. J'en suis convaincue puisque je sens un soutien que l'on n'avait jamais eu par le passé à ce sujet-là.

On a posé aussi la question des indicateurs, et cetera. Dans le cadre du programme de sécurité de l'information du SPW, on est en train de mettre en place toute une série d'indicateurs. Nous avons déjà pas mal de suivi de l'état d'avancement des projets et des activités, définis sur base des recommandations techniques ou organisationnelles faites pendant la crise. Sur base de ces recommandations, on a élaboré une série de priorités par feuille de route annuelle qui s'inscrivent dans la continuité. On a ainsi une feuille de route 2025, une feuille de route 2026 et l'on est en train de préparer la feuille de route 2027, avec toute une série de priorités sur lesquelles on a travaillé.

Mme Roucou vous a parlé des principales. Parmi celles qui ont le plus évolué depuis la crise, il y a la mise en place du SOC. Le SOC regroupe en fait énormément de mesures de NIS 2, qui ont été englobées dans ce marché et dans toutes les activités qui tournent autour, comme la révision du processus de gestion d'incident. On en a beaucoup parlé. Que se passe-t-il quand on a un incident ? Qui prévient qui ? Dans quel ordre ? Qui détecte ? Pour tout cela, on a vraiment fait un bond de maturité, notamment grâce à ces travaux sur le SOC, sur la détection et la réponse.

On a parlé aussi de sensibilisation des agents. On a mis en place cette plateforme de formation récurrente, où les agents reçoivent tous les mois une petite formation. Ils reçoivent régulièrement des campagnes de faux *phishing* pour s'entraîner à les détecter et à y répondre de manière appropriée.

On a formé aussi le *top management*. Ils ont participé aussi à des séances de formation. Comme M. Guisse l'a dit, ils sont aussi interpellés tous les mois au comité stratégique pour discuter du programme de sécurité, de ses avancées et des priorités.

On a eu aussi des formations à l'attention du personnel technique, répondant à un besoin de formations plus pointues sur des choses spécifiques, en particulier pour les experts du SPW Digital.

Concernant l'IA, cela peut être très positif comme cela peut être plutôt risqué. L'IA amplifie un certain nombre de risques ou les rend plus probables. Les attaques sont plus sophistiquées, plus fréquentes et plus récurrentes. Néanmoins, l'IA peut nous servir aussi à nous aider à nous protéger contre les hackers qui pourraient l'utiliser à des fins malveillantes. C'est un de ses aspects positifs.

Nous utilisons, notamment dans notre SOC, un certain nombre d'outils qui utilisent l'IA pour aider à la détection des tentatives d'intrusion ou des incidents de sécurité. C'est une arme à double tranchant, qui nous aide autant qu'elle nous augmente nos risques. Nous intégrons cette technologie dans nos pratiques.

Je reviens un instant sur la crise. Monsieur Liradelfo, vous me demandiez si 100 % étaient résolus. Oui, nous avons estimé que, fin décembre de l'année passée, le projet de restauration du système d'information avait été clôturé parce que 100 % des activités qui dépendaient de l'IT et qui avaient été impactées avaient été restaurées d'une manière ou d'une autre. On n'est plus dans cette période de crise et la page est derrière nous. Cela ne veut pas dire qu'il ne reste pas des choses à faire ni que toutes les recommandations suite à la crise sont intégrées ; elles font partie de ce programme de transformation et de sécurité de l'information qui avance fort bien.

Il y avait une question aussi sur le RGPD, sur la protection des données personnelles. Dans le cadre de la crise, et notamment parce qu'un certain nombre d'informations avaient potentiellement été, pas dérobées, mais probablement rendues lisibles par notre attaquant. Effectivement, il y a les processus liés au RGPD. Le DPO a fait toutes les notifications nécessaires en la matière, que ce soit vers l'APD ou vers les personnes concernées. Ces dernières ont été informées du risque que leurs données personnelles – et lesquelles – avaient été éventuellement consultées et les risques auxquels ces personnes s'exposaient. C'était très limité, au sein de l'administration, et encore, sur des données administratives, ce qui expose les personnes principalement à du *phishing* supplémentaire. Cela explique notre politique de sensibilisation.

Vous avez posé la question des audits de sécurité. Actuellement, nous sommes en phase d'évaluation de notre maturité NIS 2 par rapport au référentiel CyFun,

dont Mme Roucou a parlé, qui est proposé par le CCB pour être accompagné dans la démarche NIS 2. Cela veut dire que c'est un audit interne. Néanmoins, des audits externes seront régulièrement réalisés par le CCB, comme prévu par la loi NIS 2. J'imagine que vous en parlerez. Nous devons faire des audits internes et nous soumettre à des audits de contrôle externes.

Il y a eu toute une série de questions plus techniques sur les vulnérabilités, les changements d'outils, VPN, mots de passe, et cetera. Ce sont toutes des activités que nous suivons de près. Je ne vais pas pouvoir vous donner de l'information sur quelles sont nos vulnérabilités, j'espère que vous comprendrez pourquoi je ne donne pas, ici et de manière publique, ce genre d'information. C'est toute une série de choses pour lesquelles nous avons différents outils qui font de l'identification de vulnérabilités qui, du fait que nous les détectons, conduisent à des processus de mise à jour des outils et des tactiques pour éradiquer ces vulnérabilités. S'il n'y a pas de mises à jour possibles, il y a des solutions alternatives pour réduire le risque et le mitiger. Du point de vue de l'utilisateur, cela explique des mises à jour, des changements de mot de passe, et cetera.

La politique de gestion des accès et gestion des mots de passe était déjà bien présente au SPW, ce qui a beaucoup évolué depuis la crise et la systématisation de ce que l'on appelle la MFA, l'authentification à deux facteurs, c'est-à-dire que quand on se connecte, on reçoit un SMS ou un appel qui vérifie que l'on essaie bien de se connecter. Ce système de double authentification est maintenant généralisé dans tous nos systèmes, tant en interne que vis-à-vis des usagers externes. Itisme est typiquement un outil d'authentification à deux facteurs permettant de vérifier l'identité de la personne qui se connecte pour autoriser l'accès. Ce sont des outils que nous n'avions pas encore généralisés et qui le sont depuis la crise.

Il y a également eu une question sur les délais légaux pendant la crise. M. Guisse y a déjà un peu répondu. Pendant la crise, la volonté était que les citoyens et les entreprises ne soient pas pénalisés par cette indisponibilité des services publics. Un arrêté du Gouvernement, si je ne me trompe pas, a prolongé les délais légaux de toute une série de procédures, ce qui a permis de...

Mme Veronica Cremasco (Ecolo). – Comme on avait une interaction, je voulais juste reformuler ma question.

J'ai bien suivi ce qui concerne les délais légaux, M. Guisse y a répondu. Heureusement, les données n'étant pas accessibles, on ne peut pas se résigner à raboter une enquête publique – et heureusement ! – ainsi que passer outre les dispositions prises, en ce compris dans les textes que l'on a votés ici au Parlement.

Comment se prémunit-on de ces fuites de données à l'avenir ? Il y a certainement moyen d'immuniser des données issues de WalOnMap qui servent une enquête publique dans le cadre d'un permis. Je ne sais pas si ces données font l'objet d'un contrat classé « Secret défense », mais elles ont un impact énorme sur le citoyen. Comment procédez-vous pour toute une série d'informations pour que cela n'arrive plus ? Pendant le Covid, des procédures de ce type ont dû être mises à jour, et c'est bien normal parce que le citoyen n'a rien demandé et il faut qu'il y ait accès.

Disposez-vous d'une gestion de votre infrastructure qui permet de déterminer que telles données sont immunisées parce qu'on sait qu'elles servent dans des procédures qui, de mon point de vue, nécessitent un respect de la vie privée, mais qui ne sont pas des informations extrêmement sensibles en matière d'attaque de l'État ou d'attaque de la Région ? Avez-vous réfléchi à cela ? Nous, qui sommes de l'autre côté de la barrière, voyons que tous les citoyens sont évidemment démunis par rapport à ces aspects et se posent plein de questions. En conséquence, on attend que le Gouvernement prenne une décision. On débat ici et l'on fait passer des textes. Ce qui m'inquiétait était que tout cela pourrait être amélioré dans la gestion du contact entre les autorités en général et le citoyen.

Mme la Présidente. – La parole est à Mme Quoilin.

Mme Isabelle Quoilin, Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital). – La réponse est variable, car elle est autant organisationnelle que technique. Il y a des choses que l'on peut imaginer organiser. Ensuite, il y a ce qui est faisable techniquement parlant, à court terme, à moyen terme et à long terme. Or, j'entends que vous suggérez de dire qu'il y a une série d'outils informatiques qui ne sont pas critiques au sens de la protection des données, et cetera, et que l'on pourrait séparer ces outils de ce qui est critique.

Mme Veronica Cremasco (Ecolo). – Soyons bien clairs. Je ne fais aucune suggestion technique. Ne me prêtez pas une solution technique ; d'ailleurs, mon collègue panique.

Mme Isabelle Quoilin, Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital). – J'essaie d'expliquer que ce que vous proposez peut être résolu par la technique.

Mme Veronica Cremasco (Ecolo). – J'en appelle plutôt à votre technicité.

Mme Isabelle Quoilin, Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital). – Cependant, si c'est possible à réaliser, c'est complexe et ce n'est pas, comme on a dit tout à l'heure, réalisable avec des yakas. Il s'agit de stratégies qui doivent se voir sur le long terme, compte tenu du fonctionnement du réseau du SPW, de l'interconnexion des systèmes, de

l'interconnexion des applications et, on l'a dit à plusieurs reprises, de l'obsolescence technologique sur un certain nombre d'équipements.

Aujourd'hui, le système est tellement interconnecté qu'il n'est pas nécessairement rapidement faisable de scinder les choses. Dans un avenir moyen-long, en fonction des priorités et des urgences, certes, c'est le genre de réflexion à prendre en compte pour séparer les choses et rendre les données accessibles à différents niveaux.

Mme la Présidente. – La parole est à Mme Roucou.

Mme Isabelle Roucou, Directrice générale du Service public de Wallonie Digital (SPW Digital). – Pour compléter, nous avons de grands programmes de transformation au niveau cybersécurité. Ce que vous mentionnez implique potentiellement des budgets phénoménaux au niveau de la Région. Cela voudrait dire que, pour toute une série de systèmes critiques – Dieu sait que, quand on parle aux métiers, chacun considère que son système est critique, mais on peut encore le phaser –, on aurait une duplication complète à tout moment, quelque part ailleurs, qui permettrait de quand même faire fonctionner le système.

Dans mon très jeune temps, j'ai travaillé chez Euroclear et je suis encore les actualités de cette société. Dans les années 1990 et 2000, Euroclear avait les moyens d'avoir un système qui ne servait à rien. Ils avaient dédoublé Bruxelles à Braine-l'Alleud à l'époque. Ensuite, ils ont commencé à l'utiliser, mais cela a représenté des millions et des millions d'investissements. Vous voyez ce que je veux dire. Dès lors, on a de belles choses à faire dans l'augmentation de la préparation à la cybersécurité, mais on doit trouver la juste mesure entre budget, sécurité, et cetera.

Tout est possible à vrai dire, tout dépend du budget que l'on pourrait y mettre.

Mme la Présidente. – Madame Quoilin, vous vouliez ajouter quelque chose ?

Mme Isabelle Quoilin, Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital). – Je m'inscris dans les vœux qui ont été formulés par mes deux collègues, M. Guisse et Mme Roucou, parce que je suis assez alignée avec eux. Donc, je vais essayer de ne pas redire la même chose qu'eux.

Selon moi, ce qui empêche aujourd'hui le plus d'avancer dans la cybersécurité au niveau du SPW, c'est l'obsolescence et la maintenance, ce qui ne dépend pas nécessairement du SPW Digital, mais qui dépend en partie du métier. Aujourd'hui, les applications sont prises en charge par les métiers et par des budgets métiers. Il est difficile d'investir dans la maintenance parce que c'est quelque chose qui ne se voit pas et que l'on ne peut pas vraiment inaugurer. C'est là où l'on a la plus grosse difficulté de faire considérer ces

investissements dans la maintenance, c'est-à-dire simplement remettre l'application à jour afin qu'elle fonctionne exactement comme aujourd'hui pour l'utilisateur, qu'il soit interne ou externe, mais que, au niveau de la technologie, ils atteignent le niveau requis pour ne plus générer de problèmes de sécurité. C'est mon premier souhait.

Mon deuxième souhait – en partie déjà réalisé –, c'est que je souhaiterais que l'on ne doive plus rejustifier chaque année le budget dont on a besoin pour la cybersécurité. Selon moi, c'est un budget structurel et récurrent. On a atteint depuis deux ans un certain niveau, mais ce niveau nous semble nécessaire et aujourd'hui suffisant pour espérer une évolution du SPW en la matière.

Mon troisième souhait – on a beaucoup parlé de fonction publique – va de pair avec les moyens structurels. Nos ressources sont surtout financées par du budget, étant donné que ce sont des ressources externes, mais c'est aussi une manière de rendre ces fonctions plus pérennes dans le temps. Il faut que les personnes qui sont là soient quelque part assurées d'être encore là demain ou, en tout cas, tant qu'on a besoin d'elles et de ne pas être tous les six mois ou tous les neuf mois en train de se dire : « Je vais chercher ailleurs parce que je n'ai pas de perspective sur le prochain contrat que l'on me donnera puisqu'il dépend du budget ». Il s'agit de rendre nos fonctions, qu'elles soient internes ou externes, attractives et de pouvoir garder les personnes de compétences que nous avons aujourd'hui.

Mme la Présidente. – La parole est à Mme Clouner.

Mme Phédra Clouner, Directrice générale adjointe de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB). – Je vous remercie pour vos questions. Je vais répondre aux questions et, si j'en oublie, n'hésitez surtout pas à me le signaler. Les détails techniques seront donnés par M. Peeters.

À quel moment le SPW a-t-il été alerté ? Comme on vous l'a dit, fin mars, on a eu des informations au niveau du CCB sur le fait que des équipements Ivanti en fin de support compromis avaient été observés en Europe. Étant donné que l'un des services du CCB est d'étudier la menace au niveau national, il a commencé à analyser les risques sur les acteurs belges par rapport à ce matériel en fin de support. Le 3 avril, des informations d'Ivanti et de Mandiant ont été divulguées sur une vulnérabilité. Le CCB a un système qui s'appelle le Spear Warning. Il a des sources qui lui permettent d'identifier des systèmes vulnérables ou infectés. Il a envoyé des alertes précoces aux organisations belges concernées par cette vulnérabilité, dont le SPW. Le 15 avril, le CCB prend contact avec le SPW, qui confirme que des activités suspectes sont signalées. Une réponse conjointe à l'incident est alors lancée. À partir du 16 avril, il y a une véritable aide

concrète qui est offerte par le CCB au SPW. Nous avons aussi un plan de crise cyber qui formalise les actions à prendre dans le cadre de la gestion d'incidents de cybersécurité. Le 17 avril, l'incident était élevé au niveau d'un incident national. À la suite des recommandations qui ont été faites par le CCB, le SPW interrompt donc la connexion à internet.

Pour répondre à la question demandant si l'interruption de la connexion à internet était proportionnée, en fonction des informations qui étaient disponibles, la réponse est oui. Nous tenons à insister sur le fait que c'est une décision courageuse. Pourquoi ? Parce que, souvent, les victimes de cyberincidents hésitent à couper internet pour continuer à offrir un service. Dans ces conditions, la cyberattaque continue à se propager dans les systèmes. Comme je l'ai dit tout à l'heure, si l'on n'avait pas pris cette décision, ce se serait propagé et aurait pris des proportions complètement ingérables. Bravo pour cette décision courageuse sur nos conseils !

Une autre question portait sur la complexité et la gravité de l'incident. On l'a bien compris avec les informations données par le SPW, le FCCU et nous-mêmes, cet incident était complexe, parce qu'il concernait un certain nombre de systèmes et énormément d'applications. Cette organisation décentralisée ne facilitait pas les choses. Un certain nombre de serveurs et d'applications ont été touchés par cet incident. L'incident a été grave. La gravité de l'incident est avérée et a été traitée par le SPW, avec le support des différents acteurs.

Que ma collègue n'hésite pas à m'interrompre pour compléter ou si je dis des bêtises.

Au niveau de la question sur le niveau d'expertise qui correspond aux bonnes pratiques, il est assez difficile au CCB de répondre à ce genre de question, parce que nous n'avons pas une vue complète sur toute l'expertise qui est à disposition au niveau du SPW. Par contre, il est utile de mettre en évidence que le SPW a fait appel au CCB. C'est une entité NIS 2, donc ils sont un peu obligés de notifier le fait qu'ils ont été victimes d'incidents, mais cela a été fait de manière totalement spontanée. Ils ont eu l'intelligence de s'entourer d'experts externes pour les aider à gérer cet incident, que ce soit Microsoft ou des prestataires IT.

À côté de cela, la question de l'expertise en matière de cybersécurité a été déjà soulignée à plusieurs reprises, surtout quand on voit l'évolution très rapide des technologies. C'est quelque chose qui s'entretient très rapidement, plus que pour n'importe quel type d'autres profils, irais-je jusqu'à dire.

Les dispositifs indispensables pour ce genre d'organisation étaient-ils mis en place ? Les recommandations émises, tant par la police que par le CCB et Microsoft, indiquent que certains dispositifs

pouvaient déjà être partiellement présents, mais pouvaient être optimisés. C'est aussi ce qui a été mis en évidence par le SPW : ils ont pris tout ce qu'ils pouvaient prendre des *lessons learned* de cet incident, ils ont répondu à certains manquements, certaines choses qui pouvaient être optimisées suite à cet incident.

Un des objectifs du CCB est de mettre à disposition des entités NIS 2 des recommandations liées à cet incident, mais aussi des recommandations plus globales pour atteindre un niveau de cybersécurité adéquat qui correspond aux exigences de NIS 2, ces fameux référentiels de sécurité CyFun qui, comme cela a été dit par Mmes Quoilin et Roucou, sert maintenant de feuille de route au SPW pour augmenter son niveau de sécurité. Tant mieux, parce que, dans le cadre de l'implémentation de la loi NIS 2, les entités NIS 2 doivent se faire certifier sur base d'un référentiel de sécurité, que ce soit le CyFun ou l'ISO 27001, mais plus spécifiquement le CyFun. Or, pour se faire certifier, il faut atteindre le niveau de cybersécurité adéquat. Ce n'est d'ailleurs pas le CCB qui certifie – je suis désolée –, mais ce n'est pas grave, on continuera à collaborer. C'est un organisme accrédité par BELAC, l'autorité nationale d'accréditation, qui organise les audits permettant d'obtenir la certification nécessaire dans le cadre de l'implémentation de NIS 2. Par contre, le CCB intervient par la suite pour constater le fait que les organisations ont bien mis en place toutes les mesures qui devaient l'être.

On m'a demandé si le SPW disposait des moyens nécessaires. Objectivement, nous n'avons pas de visibilité sur tous les moyens qui étaient disponibles à l'époque. Nous connaissons les moyens qui ont été mis à disposition à la suite de l'incident, mais nous n'avons aucune visibilité sur ceux qui étaient disponibles ou nécessaires pour le SPW à l'époque. À présent, un certain budget a été libéré. Je me permets d'ailleurs de rebondir sur ce qui a été dit : mettre en place de la cybersécurité de manière pérenne, ce n'est jamais un *one-shot*. Il faut donc effectivement un budget structurel pour assurer cette cybersécurité, surtout au vu de l'évolution de la cybermenace.

Quant à d'éventuelles recommandations majeures qui seraient en suspens, d'après les explications qui nous parviennent aujourd'hui, le SPW a vraiment pris au sérieux les recommandations édictées par la police et par le CCB et il est en train de mettre en place les mesures nécessaires pour les respecter. Comme cela a été dit, ce genre de choses ne se fait pas d'un coup de baguette magique. C'est quelque chose qui doit se faire sur le long terme et une priorisation doit être envisagée dans le cadre de la feuille de route du SPW. À ce sujet, nous, à partir du moment où les recommandations qui sont explicitées dans le référentiel de cybersécurité sont suivies, c'est ce qui nous importe.

En ce qui concerne la coopération entre le CCB et les entités fédérées, la bonne nouvelle, c'est qu'elle est

excellente, comme vous avez déjà pu le constater dans le cadre de la gestion de cette crise. Un plan de gestion des crises cyber a été établi avec les différents acteurs, entités fédérées comprises, et le rôle de ces dernières dans ce contexte spécifique a été défini. À côté de cela, nous avons également une collaboration avec l'Agence du numérique dans le cadre de la mise en place de sa CERT – Cyber Emergency Response Team – régionale. Nous mettons aussi en place une coopération plus globale, pas spécifiquement sur la gestion des incidents, mais sur la gestion de la cybersécurité. Au niveau national, nous avons une plateforme, le NCC-BE, qui reprend aussi les entités fédérées pour que l'on puisse échanger sur les bonnes pratiques en matière de cybersécurité et sur les projets aux niveaux fédéral et régional.

Par contre, ce que l'on aurait pu aussi constater lors de la gestion de cet incident, c'est que l'on aurait peut-être pu mieux optimiser la communication entre les centres de crise respectifs. En effet, on s'est rendu compte que le centre de crise régional flamand n'était pas tout à fait au courant de ce qui se passait. Or, une crise cyber à un endroit peut parfois avoir un impact ailleurs. Ce n'est pas comme le nuage de Tchernobyl, cela ne s'arrête pas aux frontières, et cela peut avoir un impact sur les autres Régions.

Certains ont demandé si NIS 2 modifie le niveau d'exigence auquel une administration doit répondre. Oui, c'est pour cela que la directive et la loi NIS 2 ont été mises en place. Les entités NIS 2, face à la recrudescence et à l'évolution de la cybermenace, se doivent maintenant de structurer et formaliser leur politique de cybersécurité. Comme on l'a vu dans la directive NIS 2 – c'est assez intéressant dans une directive –, il y a des éléments relativement techniques, en définitive, qui sont repris dans celle-ci, quand on parle de gestion d'incident, d'installation et d'authentification multifacteur et ce genre de choses. Oui, mais cette directive NIS 2 n'est pas là dans une optique de *pure compliance*, elle est là aussi pour faire face à une menace cyber qui est de plus en plus importante et qui ne baissera pas, que les choses soient claires.

Par ailleurs, la bonne nouvelle est que la mise en place et l'entrée en vigueur de NIS 2 a fait en sorte que le CCB offre des services supplémentaires par rapport à l'implémentation de cette directive NIS 2. On parlait du référentiel de sécurité CyFun, qui a pour but d'aider les organisations à acquérir un niveau de maturité, mais aussi à prioriser leurs investissements. C'est très important. Nous avons aussi des services, comme Early Warning System, des outils d'évaluation de la maturité, qui peuvent être utilisés par les organisations NIS 2, donc par le SPW. Si j'ai bien compris, c'est tout à fait le cas.

Au niveau des principales menaces, comme on l'a vu depuis quelques années, on a des types de menaces

qui sont récurrents. Ce sont les *ransomwares*, les comptes compromis et ce genre de choses. On a également les attaques DDoS. Vous parliez notamment du Parlement de Wallonie qui avait été victime d'une attaque DDoS. On voit également un lien de la menace avec la situation géopolitique. Reprenons ces fameuses attaques DDoS, où l'on a constaté qu'il y avait une recrudescence de ces attaques chaque fois qu'une déclaration politique pour l'Ukraine, par exemple, était faite.

À côté de cela – on en a beaucoup parlé et l'on en parlera encore beaucoup –, il y a l'intelligence artificielle. Cette dernière a déjà un impact sur la cybermenace. On peut parler de l'intelligence artificielle en tant que telle, qui peut effectivement aider à rendre des campagnes de *phishing* qui sont plus crédibles, qui peuvent aider à scanner plus facilement les systèmes et ce genre de choses. Cependant, ce que l'on entend aussi depuis le mois d'avril, c'est ce qui a trait à l'intelligence artificielle avancée. Cela représente un vrai challenge, parce que cela permet vraiment d'identifier beaucoup plus rapidement les vulnérabilités dans les systèmes, et même des vulnérabilités qui n'avaient jamais été identifiées précédemment. C'est une menace que l'on se doit de prendre excessivement au sérieux – le SPW est conscient de cela – et qui change également la manière de gérer la cybersécurité. Comme on trouve très rapidement des vulnérabilités, cela veut dire qu'il faut faire très rapidement les mises à jour dans les systèmes, par exemple.

Par contre, la bonne nouvelle – on est là dans l'optique que c'est horrible et que tout le monde va l'utiliser pour lancer des cyberattaques – est que ce genre de modèle est utilisé aussi par les experts en cybersécurité et par le CCB pour protéger nos organisations les plus critiques par rapport à la menace.

Ce qui est implémenté au niveau SPW correspond-il aux standards attendus ? C'est un peu tôt pour répondre à cette question, parce que le SPW est pour le moment dans son travail d'évaluation de sa maturité par rapport à CyFun. Merci pour cela. Pour le moment, tant que l'évaluation de sa maturité n'est pas finalisée, il est difficile d'avoir une réponse définitive à la question : « Cela correspond-il aux standards attendus ? »

On parlait de tout ce qui est détection de vulnérabilités notamment. J'en ai déjà très rapidement parlé. Cependant, le CCB a deux systèmes spécifiques pour aider les organisations à identifier, mais aussi à mitiger les vulnérabilités qui sont identifiées – vulnérabilités, mais aussi systèmes infectés, ce genre de choses –, dont l'ESP *warning*. Cela veut dire que, avec les sources et les outils qui sont à notre disposition, on arrive à identifier des systèmes qui sont affectés ou qui sont vulnérables et à prévenir les organisations de manière proactive. Nous ne sommes pas simplement dans la réaction, c'est toute la beauté de l'histoire. À côté de cela, le CCB met à disposition une plateforme

qui s'appelle l'Early Warning System, qui m'envoie des alertes et des informations sur les menaces en tant que telles – le SPW est un utilisateur de cette plateforme. N'hésitez pas à me le dire si j'ai oublié quelque chose d'important.

Mme la Présidente. – La parole est à M. Peeters.

M. Jean-Luc Peeters, Directeur de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB). – J'ai fait exprès de ne pas répondre et de ne pas te corriger, comme cela j'avais encore quelque chose à dire.

J'ai cru comprendre une question par rapport à ce que l'on fait pour les opérateurs non-NIS 2. Il faut signaler que dans les discussions que l'on a avec le CRT wallon – on essaie d'éviter que l'on fasse trop doublon l'un avec l'autre –, une des approches, c'est qu'ils vont regarder les opérateurs ou les entités non-NIS 2, comme les communes, et cetera. Quand nous recevons des questions au niveau des communes pour une assistance dans le cadre d'une attaque de cybersécurité, le CCB donne un coup de main, mais les moyens déployés, en fonction des priorités ou du nombre d'incidents, seront forcément différents avec un acteur comme le SPW ou une certaine commune. A priori, on essaie de voir. Par exemple, les hautes écoles ou les universités sont aussi clairement dans le *scope* de ce que le CRT wallon est occupé à mettre en place comme système.

Par rapport à la partie vulnérabilité, tu as été relativement exhaustive. Sur le fonctionnement, il faut bien se dire que nous nous positionnons en complément des systèmes existants. On a des systèmes pour détecter les vulnérabilités. On essaie d'avoir une sorte de matrice d'évaluation d'une vulnérabilité quant à l'impact potentiel et à l'éventualité d'être exploité. Si, en fonction de cela, on a une évaluation qui dit que c'est potentiellement quelque chose d'important ou de dangereux – on est occupés à travailler quotidiennement sur ce type de dossier –, nous allons encore entreprendre des actions supplémentaires, comme un *scanning* spécifique au niveau des organisations de la Belgique, une identification.

Je voudrais parler d'un point important pour votre contexte : une des difficultés que nous rencontrons très souvent avec les fournisseurs, c'est la non-volonté de donner ou de divulguer des informations quant à leurs clients. Je peux comprendre jusqu'à un certain niveau, mais quand on est dans le type d'action où une vulnérabilité est exploitée et que l'on n'est pas capable d'identifier un opérateur économique – même si l'on a heureusement certains moyens légaux qui nous permettent d'identifier des adresses IP qui ont été encadrées par rapport à cela –, ce n'est pas le Valhalla non plus. Il faut savoir que, depuis le 11 septembre, il y a le nouveau règlement, le CRA – Cyber Resilience Act – qui donnera l'obligation au niveau des fabricants software et hardware, au niveau cybersécurité, à partir

du moment où des vulnérabilités sont utilisées ou exploitées, de notifier cela via une plateforme unique où chaque CSIRT – le CERT, SiteRisk, le CCB – aura l'information et pourra la divulguer par rapport aux différents acteurs européens. Ce n'est certainement pas une solution miracle, mais c'est une pierre à l'édifice qui va nous aider beaucoup.

Par rapport à la partie sur la peur de l'IA, il faut être très prudent. Phédra a très bien expliqué la problématique. On a un programme qui s'appelle Coordinator Responsible Disclosure : ce sont des hackers éthiques qui peuvent notifier des vulnérabilités, en complément aux obligations légales et qui, s'ils suivent toute une procédure bien spécifique, peuvent avoir une protection juridique. Si l'on regarde, rien qu'au niveau des chiffres, on a déjà deux fois plus de vulnérabilités qui nous ont été rapportées comparativement à la même période l'année passée. C'est clairement grâce à l'intelligence artificielle. Elle est un risque, mais si elle est bien utilisée, elle peut servir à mieux sécuriser les systèmes. De toute façon, nous devons l'utiliser, il n'y a pas le choix. Nous nous attendons à voir une augmentation relativement importante dans les deux années à venir, pour après se stabiliser parce que ces outils vont forcément aider à mieux sécuriser. Quand on est dans la défense, un attaquant doit trouver une seule porte d'entrée ; quelqu'un qui défend les systèmes doit regarder toutes les portes d'entrée possibles et imaginables. Le job est parfois un tout petit peu différent.

Une toute dernière clarification au niveau du *pentesting*, car c'est certainement très important. Ce n'est pas suffisant, mais complémentaire à toute une série d'autres actions. Une des actions est une veille permanente au niveau des systèmes qui sont, par exemple, exposés sur internet pour voir si de nouvelles vulnérabilités sont sorties, et cetera. L'intelligence artificielle peut le faire parce que, quand on voit les systèmes exposés, les développements et les librairies – sans rentrer dans les détails techniques – qui sont utilisés par rapport à cela, c'est quelque chose d'excessivement compliqué. Si l'on n'utilise pas des outils automatiques pour le faire, un être humain n'est pas capable d'assimiler la masse de données par rapport à cela.

Mme la Présidente. – La parole est à Mme Derkoningen.

Mme Kris Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU). – Concernant le rôle de notre service, nous ne sommes pas le CCB. Ce dernier est là pour donner une réponse à l'incident là où la police va intervenir pour préserver les traces et mener l'enquête par la suite. Nous, on va rechercher les auteurs pour essayer de faire en sorte que, dans le futur, ils ne pourraient plus nous faire du mal ou refaire une attaque cyber. Voilà notre rôle.

On a quand même des permanences pour tout cela : au niveau de la police fédérale et de la FCCU, nous avons des enquêteurs digitaux qui sont de permanence pour ce genre de faits. Cela s'appelle la QRF – Quick reaction force. Le but est d'essayer de les impliquer par rapport à des attaques cyber en cours pour essayer de descendre sur place au moment même et pour préserver les traces sans ralentir pour autant l'enquête ou la réponse sur l'incident. Pour cela, on travaille très bien avec le CCB ; on a une très bonne entente par rapport à cela. On a un groupe avec des partenaires dans le cadre des cybernotifications. Ils peuvent nous prévenir par ce moyen-là. Pour le SPW, je pense que cela s'est passé de cette manière-là : le CCB était sur place, ils nous ont prévenus et l'on a convenu d'une réunion au plus vite par rapport à ce qui se passait. Il y a eu un peu de délai.

Si je devais vous faire des recommandations par rapport à cela, c'est de nous impliquer. On ne nous aime pas trop, parce que l'on n'est pas là pour vous aider dans un premier temps, mais on est là pour faire l'enquête. Notre enquête a quand même son importance. On est souvent oublié. Si j'ai un vœu à faire, c'est de nous impliquer davantage et de nous appeler.

Mme Éliane Tillieux (PS). – Pour avoir une idée, combien de temps après l'incident a-t-il fallu pour que l'on vous contacte ?

Mme Kris Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU). – On a été impliqué le 18 avril. Une réunion a été mise en place à 11 heures par le CCB, avec la victime, pour essayer de nous impliquer dans ce dossier.

Par rapport à vos questions concernant la manière de préserver les preuves et les traces, je vous conseille d'appeler ma QRF afin d'avoir les enquêteurs digitaux qui vont descendre sur les lieux pour faire le nécessaire.

Vous avez demandé si les postes administratifs étaient davantage visés par rapport aux sociétés privées. Je ne pourrais pas vous donner une réponse par rapport à cela. En effet, au niveau de la FCCU, on ne traite que des dossiers concernant des infrastructures critiques. Je n'ai dès lors pas une vue sur les chiffres des sociétés privées. Au niveau des chiffres relatifs à la cybercriminalité, beaucoup de sociétés ne nous appellent pas. Nous ne disposons donc pas du chiffre à cet égard. C'est aussi un problème : il n'y a aucune obligation de déposer plainte pour des faits de cybercriminalité.

Pour les questions d'IA, je pense que mes collègues ont déjà répondu de manière suffisante ; je ne peux que confirmer leurs propos. Ce que je peux rajouter, c'est qu'au jour d'aujourd'hui, il ne faut plus disposer de connaissances en informatique pour commettre des faits de cybercriminalité. À travers le *cybercrime as a service*, les cybercriminels mettent à disposition leurs connaissances, leurs outils et leurs infrastructures. Si

l'on prend l'exemple du RaaS – *ransomware as a service* –, il y a vraiment des kits de *ransomware* prêts à l'emploi. Vous avez le *malware*, vous avez une liste avec des cibles que vous pouvez attaquer, un *dashboard* où vous pouvez suivre le nombre d'attaques qui ont lieu, et il y a même un service clientèle après emploi pour vous aider à négocier le paiement du *ransomware*. L'IA, c'est une chose, mais la mise à disposition de ces connaissances agrandit le nombre potentiel d'auteurs de faits de cybercriminalité. Je voulais juste rajouter ces éléments, car je pense que mes collègues ont déjà bien répondu au sujet de l'IA.

Vous avez demandé comment le CCB et la police fédérale pouvaient s'organiser avant une attaque. Une bonne collaboration existe déjà entre nous, et l'on se tient au courant par rapport aux cyberattaques qui ont lieu.

Je passe aux questions du PTB. Concernant la gouvernance informatique, j'ai effectivement évoqué le fait que les différentes directions ont recours à des technologies différentes et que, par conséquent, il est difficile de disposer d'une vue globale de l'environnement informatique et de la gestion. Je ne dis pas forcément que tout le monde devrait utiliser le même système, mais je ne suis pas convaincue que le fait d'avoir des systèmes identiques rende plus vulnérable. S'il y a une bonne maintenance des systèmes, tout est possible.

Quant à savoir qui contacte qui, quelle est la procédure exacte et comment impliquer la police, vous pouvez toujours contacter la police locale. Les agents savent qu'il y a des permanences au niveau de la police fédérale pour tout ce qui concerne les dossiers cyber et qu'ils peuvent faire appel à nous pour descendre sur place. Je pense que le CCB, quand il est impliqué, dispose également d'une ligne directe vers nos services. Cela peut donc également être fait de cette manière.

La dernière question, provenant d'Ecolo, concerne l'architecture et les conseils que peut donner la police. Mes enquêteurs du digital peuvent donner des conseils, mais ce n'est pas notre mandat. On peut donner de petits conseils quand on procède aux auditions des victimes, mais ce ne sera jamais quelque chose de structurel qui sera mis en place par la suite. Ce n'est vraiment pas notre mandat.

Mme Veronica Cremasco (Ecolo). – C'est dommage, parce que vous avez des infos dont ils ne disposent pas, puisque vous êtes de l'autre côté de la barrière.

Mme Kris Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU). – Oui, mais le CCB est au courant de toutes les recommandations que j'ai données et a fait le nécessaire. Cela ne m'inquiète pas du tout. Il n'y a pas une information qui n'est pas

donnée et le CCB peut correctement renseigner la victime par rapport à cela.

Je pense avoir répondu à toutes les questions. Si ce n'est pas le cas, vous pouvez toujours me le dire.

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Merci beaucoup pour l'ensemble des questions. Je vais essayer de répondre aux questions qui m'étaient directement adressées, mais je pense qu'il y a beaucoup de choses qui ont déjà été dites par les différents intervenants, que je remercie une nouvelle fois. On va donc essayer de ne pas être trop redondants.

Concernant les compétences que le SPW mobilise en interne et en externe pour assurer ses missions de cybersécurité – pour répondre également à M. Liradelfo –, le SPW combine des compétences internes et externes. Au 23 septembre 2026, le pôle Sécurité comptait 18 membres permanents, dont quatre internes et 14 externes – si ces chiffres ne sont pas bons, l'administration me contredira –, parmi lesquels figurent deux profils juniors, trois profils intermédiaires et neuf profils seniors. Le recours à des experts répond à la rareté de certaines compétences, à l'urgence de certains besoins et aux difficultés de recrutement. Cette dépendance doit toutefois rester maîtrisée par la documentation, les clauses de réversibilité, le travail conjoint et le transfert de connaissances. Le statut public ne permet pas encore d'être suffisamment attractif pour certains profils spécialisés en IT, OT et cybersécurité. Cela a été également dit par l'administration. La réponse durable consiste donc à adapter la politique de *sourcing*, à renforcer le recrutement et la formation interne tout en conservant un recours ciblé à l'expertise externe.

Vous m'interrogez sur l'organisation du SPW et du SPW Digital au moment de la crise. J'ai déjà eu l'occasion de donner tous ces éléments de réponse. L'absence d'un directeur général du SPW Digital et d'un inspecteur général de l'exploitation n'a pas laissé un vide de pilotage. Les mécanismes habituels relatifs à la fonction publique du SPW ont été mis en place pour assurer une continuité de service et de management. Les représentants du SPW ont eu l'occasion de mettre en avant les garanties apportées pour préserver la continuité du service public. Je tiens d'ailleurs à les remercier pour les précisions et les réponses qui ont été apportées.

En ce qui concerne la cyberattaque à proprement parler, une gouvernance de crise préétablie, fondée sur le Plan régional de gestion de crise, a été activée et renforcée dès le 18 avril 2025. Sa coordination générale était assurée par le CORTEX, autour d'une chaîne

d'escalade associant les équipes techniques chargées de l'incident, la secrétaire générale de l'époque, le comité stratégique, le cabinet et, lorsque nécessaire, le Kern d'urgence avec l'appui du CCB et d'experts spécialisés.

Cette gouvernance articulait plusieurs niveaux complémentaires : une cellule IT au sein du SPW Digital pour la conduite technique et la continuité ; les coordinateurs informatiques, les responsables fonctionnels d'applications et directions fonctionnelles et d'appui pour le lien avec les métiers ; une cellule SPW chargée notamment de la communication interne ; une cellule Gouvernement pour l'information politique, la communication externe et les relations avec les partenaires ; une cellule Kern pour les décisions stratégiques.

Les équipes techniques et le CCB ont recommandé l'isolement des systèmes. Les différentes options et leurs conséquences ont été présentées au comité stratégique. Puis, les autorités administratives et politiques ont été informées et consultées avant que la décision soit arrêtée. J'entends aujourd'hui que c'était la bonne décision à prendre.

Le pilotage a donc été assuré de manière collégiale par les niveaux technique, administratif et politique compétents, sur la base de rendez-vous quotidiens structurés : stand-up de l'équipe de crise et CODIS dans les SPW à 9 heures ; réunion avec le CCB à 10 heures 30 ; Costra à 11 heures ; information des cabinets à 13 heures ; réunion Microsoft DART à 16 heures. Les décisions majeures suivent ainsi une chaîne claire : analyse et recommandation des équipes techniques et du CCB ; examen par la secrétaire générale et le Costra ; information, cabinet et arbitrage au niveau gouvernemental ou du Kern lorsque c'était nécessaire. Cette gouvernance collégiale dotée d'un leadership identifié a permis de prendre les décisions essentielles, de coordonner une équipe de crise d'environ 50 personnes actives 24 heures sur 24 pendant les premières phases et d'organiser la restauration progressive des services. La crise confirme néanmoins l'importance de fonctions dirigeantes durablement pourvues pour assurer la continuité managériale hors période de crise.

Venons-en aux fonctions critiques du SPW ainsi qu'à l'enjeu de l'attractivité des profils IT en général et de cybersécurité en particulier. Le constat de fond est malheureusement connu : le SPW éprouve des difficultés à recruter et à fidéliser certains profils spécialisés en IT, OT et cybersécurité dans un marché fortement concurrentiel. Ici aussi, la situation n'est pas propre à la Wallonie. Toutes les administrations du pays font face au même problème. Pourtant, je partage votre objectif : ces compétences doivent être considérées comme prioritaires, car elles conditionnent la capacité à maintenir les outils, à réduire l'obsolescence, à exploiter les dispositifs de sécurité et à assurer la continuité. La réponse passe par une politique de *sourcing* adaptée à la

réalité du marché de l'emploi IT 2026, à savoir renforcer l'attractivité des fonctions internes, développer les compétences, sécuriser les parcours professionnels et recourir de manière ciblée à l'expertise externe.

Il s'agit d'un des chantiers majeurs de la transformation du SPW Digital qui est en cours et nous travaillons main dans la main avec le SPW pour trouver des pistes de solutions.

Sur les budgets affectés à la cybersécurité du SPW Digital, notamment lors de la crise, une enveloppe complémentaire de 10 millions d'euros a été décidée à la suite de la cyberattaque : 8 millions d'euros pour le SPW Digital et 2 millions pour le SPW Mobilité et Infrastructures au titre des environnements OT. Pour 2025, les dépenses directement liées à la gestion d'urgence représentaient 2,416 millions d'euros engagés et 1,905 million d'euros liquidés. Les mesures de sécurité accélérées ou structurelles représentent 8,786 millions d'euros engagés et 5,197 millions d'euros liquidés. Au total, le référentiel disponible fait donc état de 11,202 millions d'euros engagés et de 7,102 millions d'euros liquidés, en combinant l'enveloppe complémentaire et le budget de base du SPW Digital. L'écart entre l'engagement et la liquidation s'explique simplement par le calendrier d'exécution, la livraison et le contrôle de facturation.

Pour 2027, l'administration a formulé une demande de 14,311 millions d'euros pour le SPW Digital. Je défends cette demande dans le cadre des discussions actuelles du conclave budgétaire, mais aucun montant ne peut être présenté comme acquis avant l'arbitrage définitif. La soutenabilité suppose de distinguer les investissements de transformation des dépenses récurrentes nécessaires pour exploiter et maintenir les capacités. Le besoin structurel est estimé par l'administration à environ 10 millions d'euros à 12 millions d'euros par an.

D'une manière générale, les propositions en la matière sont élaborées par l'administration à partir de besoins identifiés. Ces propositions sont ensuite examinées dans le cadre de la procédure budgétaire, soumises au contrôle requis et arbitrées par le Gouvernement. Pour 2026, un budget de 11,172 millions d'euros en crédits d'engagement qui ont été prévus pour la cybersécurité du SPW Digital. Ces chiffres doivent toujours être présentés en précisant leur périmètre et en distinguant demandes, crédits accordés, engagements et liquidations.

Concernant précisément le coût du recours à Microsoft DaRT et, plus largement, à la consultance mobilisée à la suite de la cyberattaque, un montant de 2,416 millions d'euros a été engagé en 2025, dont 1,905 million d'euros a été liquidé. Ce montant regroupe les coûts informatiques directement liés à l'urgence, notamment Microsoft DaRT et le socle

d'urgence, le remplacement du VPN et la reconstruction de l'Active Directory. Les chiffres communicables doivent rester suffisamment agrégés pour ne pas exposer l'architecture de sécurité ni des informations commercialement sensibles.

Sur les enseignements qui doivent encore être traduits et les actions concrètes à la suite de la crise, de mon point de vue, les enseignements doivent se traduire par une gouvernance plus claire, une connaissance plus complète des actifs et des risques, une meilleure articulation entre les métiers et l'IT, ainsi qu'une préparation opérationnelle renforcée. Cela implique de finaliser des plans de continuité et de reprise, d'identifier les interdépendances critiques, de tester régulièrement les procédures, d'accélérer le traitement et l'obsolescence, et de professionnaliser la gestion des incidents. La trajectoire NIS 2 et l'évaluation fondée sur CyFun doivent permettre d'objectiver les écarts, de hiérarchiser les remédiations et de construire une programmation pluriannuelle réaliste. Le principal enseignement est que la cybersécurité constitue une responsabilité collective et un effort permanent, et non une action ponctuelle déclenchée après une crise.

Quant au tableau de bord non sensible, pourrait-il être transmis régulièrement au Parlement, reprenant notamment les investissements réalisés, l'état d'avancement des audits et les principaux résultats de la trajectoire NIS 2 ? Vous aurez compris que cette question est relativement sensible. Dès lors, sous réserve d'une validation de nos experts internes et du CCB, un tableau de bord consolidé et non sensible peut constituer un outil utile de contrôle parlementaire. Il pourrait présenter les moyens engagés et liquidés par grandes finalités, les principaux jalons du programme de sécurité, l'avancement des audits, l'évaluation de NIS 2, les actions correctrices prioritaires, les exercices réalisés et les indicateurs de maturité suffisamment agrégés.

Pour être fiable, chaque indicateur devra être défini, daté, assorti d'un périmètre et d'une méthode de calcul. En revanche, ce tableau de bord ne devrait pas exposer les vulnérabilités précises, les actifs critiques, les niveaux détaillés de couverture, les règles de détection, ni l'architecture de défense. Pour le reste, le SPW a répondu longuement en détail aux questions posées par Mme Cremasco et M. Liradelfo notamment. Je reste à la disposition de la Commission. Il y a déjà eu énormément de questions parlementaires sur le sujet. Je terminerai en remerciant, une nouvelle fois, tous les services qui ont été disponibles aujourd'hui pour répondre à toutes vos questions.

Mme la Présidente. – La parole est à Mme Tillieux.

Mme Éliane Tillieux (PS). – Tout d'abord, je voudrais remercier et dire tout l'intérêt de ces auditions pour mieux comprendre et cerner l'amplitude du travail réalisé ainsi que les risques que l'on tente de maîtriser au maximum, en fonction de nos moyens.

Madame la Ministre, il est vrai que rien n'est fait avant le conclave. Vous avez entendu ici la nécessité de pérenniser les moyens. Ce message, on le réitère et on le soutient grandement.

Sur la restauration après l'attaque, on a vu les progrès engrangés au niveau de l'administration. On a vu aussi les contacts noués entre vous, le CCB et peut-être encore d'autres instances. Au niveau gouvernemental, il y a une nécessité de comprendre cette logique de travailler ensemble.

Ici, on n'a pas parlé des UAP, mais il serait dommage de répéter des investissements dans les UAP pour des systèmes de protection qui vont être mis en œuvre au niveau du Service public de Wallonie, pour une administration qui a été touchée et qui connaît aujourd'hui toute la sensibilité. Je voudrais lancer cet appel. Cela dépasse largement le cadre de notre Commission, mais ce sont des moyens publics. Tant qu'à faire, autant qu'ils soient alloués au plus près des besoins, en étant inclusifs par rapport aux besoins des autres unités publiques d'administration.

Sur le *reporting* après l'attaque, vous avez cité une série de communications, de rapports, de crises, de tableaux de synthèse, et cetera. Ce qui serait intéressant – Madame la Ministre, vous venez d'en parler –, c'est un tableau de bord qui nous permettrait de suivre, au niveau du Parlement, l'allocation des ressources informatiques et de voir comment les choses évoluent à cet égard. On répond positivement à votre proposition, bien sûr version purgée des éléments trop sensibles, cela va de soi.

Sur les moyens, il me semble nécessaire de mettre les moyens suffisants. On ne peut pas dire que l'on a débloqué des enveloppes particulières pour assurer le coup après la cyberattaque, puis se dire que l'on est tranquille maintenant. Non, on va malheureusement devoir octroyer plus de moyens à l'avenir. Je dis « malheureusement » parce que ce sont des moyens qui ne seront pas alloués ailleurs. Il faut plus de moyens pour la sécurité, et celle-ci est désormais également cyber. C'est incontestable. Cela passera aussi par la formation des agents, la sensibilisation, les tests, et cetera, ainsi que par le suivi des développements technologiques et de l'intelligence artificielle qui nous réservent encore pas mal de surprises.

Sur la stratégie NIS 2, vous avez largement expliqué ce qui existe ou ce qui est en train d'être mis en place. Nous suivrons cela avec une grande attention.

Je ne vais pas poser de questions complémentaires. J'en aurai encore, mais je pense que l'heure avance, que nous avons encore du pain sur la planche au niveau de la commission et que s'il y avait des éléments plus statistiques, je poserais des questions à Mme la Ministre de manière écrite pour avoir un peu plus d'informations.

Un point que l'on n'a pas abordé, ce sont les effets concrets sur les usagers. S'il y a quelque chose d'important, c'est la formation des agents. Pour les usagers, je pense qu'il y a certainement une lorgnette que nous pourrions prendre par rapport à leur impact et à leur éveil à toutes ces questions. Cela se voit évidemment plus directement dans le secteur bancaire parce que, là, il y a des effets directs. Quand le compte commence à diminuer, l'on se rend compte que l'on a été hacké et que l'on a été imprudent. Par rapport aux utilisateurs de services publics, il y a peut-être une analyse à mener de ce côté. Elle n'est peut-être pas fondamentalement prioritaire par rapport au fait de protéger nos propres outils, mais c'est sans doute un aspect qui devra éveiller l'attention dans l'avenir proche.

Voilà ce que je souhaitais rapidement mettre en avant. J'ai encore pas mal de questions, mais je ne vais pas allonger la sauce aujourd'hui. Je vous remercie vraiment pour toutes les réponses que vous avez pu donner, avec beaucoup de précision et parfois aussi beaucoup de concision. Je vous remercie beaucoup pour cet effort.

Mme la Présidente. – La parole est à M. Massaki Mbaki.

M. Chris Massaki Mbaki (MR). – Pour être très pratique, notamment sur les paiements et la fiscalité, je crois que, sur le terrain, c'est ce qui s'est aussi ressenti. Des retours que l'on a pu recevoir, c'est que le citoyen, que ce soit pour le précompte immobilier ou autre, a pu voir une certaine souplesse de la part de l'administration. Je crois qu'il est important de le souligner.

Personnellement, j'ai travaillé dans le privé avec des systèmes tels que Microsoft au niveau des ERP, c'est-à-dire des systèmes intégrés. Au niveau de la fonction publique, on a eu un rapport de la Cour des comptes sur les frais de consultance. C'est une grosse difficulté parce que l'on est toujours partagé entre l'importance d'externaliser et le coût que cela demande. C'est un travail à faire en collaboration avec le politique pour trouver un équilibre. À chaque fois, on part dans de grosses stratégies avec des sociétés de consultance sans forcément avoir toutes les garanties d'arriver à certains objectifs. Derrière, contrairement à une société de consultance dans le privé, lorsqu'on fait une erreur, c'est la société qui paie. Au niveau de la fonction publique, ce sont des deniers publics qui sont parfois gaspillés. Néanmoins, il était important d'en parler.

Madame Quoilin, vous avez parlé de l'obsolescence et de la maintenance au niveau du budget métier. On aimerait bien, en tant que politique, ne pas regarder les budgets, mais on a cette réalité. N'hésitez pas à venir à notre rencontre parce qu'il est important pour nous, en tant que parlementaire, d'avoir vos réalités pour mieux comprendre pourquoi certains budgets doivent être

alloués. De manière générale, le SPW a pris au sérieux l'ensemble des recommandations qui ont pu être données et le CCB a bien alerté le SPW, qui a agi en conséquence.

Par rapport à la coopération avec les homologues flamands ou au niveau du *benchmarking*, je ne sais pas ce qui s'est fait avec les autres pays. En effet, d'autres pays pourraient connaître ce même type d'attaque ou, inversement, la Belgique pourrait être pionnière, subir pour la première fois une attaque et réagir de la bonne façon.

Je vous remercie pour les informations et je resterai attentif à mieux comprendre vos réalités.

Mme la Présidente. – La parole est à M. Liradelfo.

M. Julien Liradelfo (PTB). – Je remercie l'ensemble des intervenants pour les explications et les échanges que l'on a pu avoir. Il est très intéressant de savoir comment tout cela s'est déroulé, de mieux comprendre le fonctionnement de leurs services et de voir les liens qu'ils ont les uns avec les autres. J'ai eu toutes les réponses aux questions que j'ai posées en commission. Si l'on en a d'autres, on y reviendra en question écrite.

Je vais soutenir l'appel du SPW sur le besoin d'avoir des moyens à la hauteur des enjeux. Investir dans la cybersécurité peut avoir un coût, mais une attaque peut aussi avoir un coût et parfois beaucoup plus important. Il est donc important d'avoir des budgets suffisants.

Je suis content d'apprendre qu'un outil nous permettra d'avoir un suivi parlementaire puisque nous l'avons déjà demandé il y a plusieurs mois. Avoir un suivi, sans avoir tout ce qui est critique dans cet outil, pour permettre aux parlementaires d'exercer leur contrôle est nécessaire.

Mme la Présidente. – La parole est à M. Bastin.

M. Jean-Paul Bastin (Les Engagés). – Je remercie chacune et chacun pour les différentes réponses, d'avoir pris la peine d'essayer de les identifier et de les noter, puisqu'il y en avait beaucoup, et d'avoir essayé de systématiquement leur donner une réponse.

J'ai bien noté que l'attaque d'avril 2025 avait servi de piqure de rappel chez certains ou d'élément déclencheur auprès d'autres. Ce n'est pas simplement une question théorique, car cela devient désormais quelque chose de très pratique et de très concret. C'est une nouvelle réalité avec laquelle nous devons malheureusement vivre et évoluer.

Mme la Présidente. – La parole est à Mme Cremasco.

Mme Veronica Cremasco (Ecolo). – Je vous remercie toutes et tous pour vos réponses. En effet, vous

les avez passées quasiment toutes en revue, ce qui fait plaisir. Nous voyons que vous considérez le débat parlementaire. Merci aussi pour l'outil qui sera à disposition. Je pense que la grande leçon que nous retenons, c'est qu'il faut continuer à investir ; être face à la crise, avoir un *one-shot* et puis laisser tomber, ce n'est pas possible. Il faut vraiment entretenir la cybersécurité et la gestion du risque en général. J'ai bien entendu que Mme la Ministre s'était engagée à défendre cela auprès du Gouvernement pendant le conclave budgétaire. Nous verrons ce qu'il en ressort.

Vous le savez, c'est un débat qui est assez aigu en termes de contrats internes et externes, parce que c'est spécifique à ce secteur-là – d'ailleurs, tout le monde a posé des questions là-dessus. Ainsi, il y a une tension par rapport à cela. Vos réponses étaient intéressantes et marquent la réalité. Elles disent que l'on ne peut pas rester sans contrat et qu'il vaut mieux quelqu'un du privé qu'une place vide, surtout dans le contexte actuel où l'on est attaqué toutes les deux secondes. Nous continuerons certainement dans ce Parlement – vous êtes les bienvenus justement pour faire toutes les suggestions possibles – pour faire en sorte qu'il y ait un autre équilibre, parce que cela ne peut qu'induire des tensions. C'est une réalité des faits actuellement, mais il y a certainement moyen de combler. J'ai entendu que même M. Massaki Mbaki le relevait. C'est dire s'il faut rééquilibrer cela ou en tout cas y travailler.

Par rapport à la sensibilisation, j'ai un peu la même demande. Vous me dites : « Si si, c'est fait ». Donc, je me dis : « Super ! » Mon idée, c'était de vous demander, au SPW Digital en tant que tel, si la sensibilisation de tous les agents vous semble suffisante. Je ne parle pas des agents d'un secteur ou d'un autre, d'un métier ou d'un autre. Si jamais, n'hésitez pas non plus à le relayer au Gouvernement, même si, au Parlement, cela nous ferait plaisir aussi. Nous sommes nombreux à être conscients du fait que c'était autant de points d'entrée dans le système et que la sensibilisation demande des moyens, qu'il faut mettre en œuvre.

Par ailleurs, il y a un outil qui m'intéresse particulièrement et dont vous avez parlé au moment de la gestion de la crise. Moi, ce qui m'inquiétait, c'était d'abord de voir comment on testait la vulnérabilité. Merci d'avoir répondu concernant le CCB, le FCCU, le niveau fédéral, la police ou autre. Cela m'inquiète vraiment : teste-t-on en permanence la vulnérabilité du système ? Comment apprécie-t-on le risque ? Pour l'avoir vécu de plus près sur d'autres dossiers et d'autres catastrophes gravissimes comme les inondations, gérer le risque vient en plus de gérer la crise. Là-dessus, je sens des éléments, mais je n'ai pas complètement la réponse à ma question.

Ce qui m'intéressait, c'était le CORTEX, soit cet outil qui a été généré après les inondations pour gérer et évaluer le risque. Chacun a ses sensibilités, mais, moi, c'est la dimension qui m'intéresse le plus, parce que

gérer le risque, c'est essayer d'éviter la crise. Après, il faut gérer la crise aussi. C'est pour cela que je posais toutes ces questions, comme sur les *pentests*. Ce sont les bêtes moyens que moi je connais. Je demandais aussi comment le FCCU collaborait. Je comprends que l'on ne mette pas cela à plat ici. Je reviendrai avec d'autres questions, mais j'espère que la gestion du risque est aussi bien prise en considération à l'aune de ce que cela représente. Vous avez néanmoins donné des éléments de validation par rapport à cela, et je voulais juste souligner encore une fois.

Je reviendrai sur cette collaboration avec le CORTEX, Madame la Ministre. Je pense que c'est hyper important et je suis sûre que vous avez plein d'idées pour mieux faire fonctionner les choses. Surtout, ne prenez pas en considération mes idées techniques, mes idées politiques peut-être, mais pas mes idées techniques ; vous pouvez oublier.

J'ai bien entendu votre réponse et j'ignorais que c'était à ce point compliqué techniquement. J'ai été éclairée aujourd'hui sur le fait que les cyberattaques, à l'égard du SPW et des administrations, étaient tout sauf négligeables. C'est énorme, et c'est évidemment une part de la sécurité de l'État qui est non négligeable.

Ces administrations ont, par définition, toute une série de données. M. Guisse l'a bien rappelé au début en disant : on a pu stopper cela, pas cela. Une série de données sont bêtement factuelles et utilisables – pas bêtement, parce qu'elles servent le citoyen tous les jours. Je comprends que vous ayez dû couper internet et le réseau pour être sûr que cela ne s'étende pas. Néanmoins, toutes ces données, y réfléchit-on ? On me dit : « Non, c'est complexe techniquement ». Je ne prétends pas du tout avoir le millième de votre connaissance scientifique. C'est pour cela que je viens aux renseignements.

Dans toute la réorganisation de ce système, avec ces différents métiers, avec des systèmes informatiques liés aux métiers dès leur conception – c'est important, en refaisant tout cela, de le faire dès l'origine –, ne penserait-on pas à isoler ces données, ne fût-ce que pour que cela continue à rouler ? La majorité des informations sont maintenant numériques. J'entends que ce n'est pas si simple. Je n'ai pas dit que je croyais que c'était simple. Je vous ai demandé, et vous me répondez non.

C'est le service aux citoyens. Je faisais le lien : administration fort concernée, du coup, service aux citoyens, du coup, ne peut-on pas préserver une partie des données pour que cela continue à tourner, même en période de gestion de la crise réelle ?

Merci beaucoup d'être venus. J'espère que vous vous manifesterez à nouveau sur toutes ces thématiques, parce que l'on sera tout ouïe.

Mme la Présidente. – Il me reste à mon tour à remercier tout le monde : nos intervenants pour leur présentation, les collègues pour toutes leurs questions et Mme la Ministre pour ses éclaircissements.

Confiance au président et au rapporteur

Mme la Présidente. – À l'unanimité des membres, il est décidé de faire confiance à la présidente et aux rapporteurs pour l'élaboration du rapport.

La séance est suspendue.

- La séance est suspendue à 18 heures 3 minutes.

REPRISE DE LA SÉANCE

- La séance est reprise à 18 heures 7 minutes.

Mme la Présidente. – La séance est reprise.

INTERPELLATIONS ET QUESTIONS ORALES

Question orale de M. Stéphane Hazée à Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « le cadrage budgétaire de la réforme des mandats »

Mme la Présidente. – L'ordre du jour appelle la question orale de M. Hazée à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « le cadrage budgétaire de la réforme des mandats ».

La parole est à M. Hazée pour poser sa question.

M. Stéphane Hazée (Ecolo). – Madame la Ministre, j'essaie de ne pas venir à chaque fois pour ne pas sembler vous harceler. Ici, c'est par question écrite que je vous répondais, mais quand plusieurs semaines s'écoulaient sans réponse, je suis alors contraint de vous interroger oralement.

J'ai eu l'occasion de vous interroger en date du 29 juin 2026, en commission, relativement au cadrage budgétaire de la réforme des mandats. Je l'ai déjà fait plusieurs fois antérieurement. Vous n'avez toutefois pas répondu à la plupart des questions soulevées et j'ai été contraint de les réitérer par voie écrite et, à présent, par voie orale.

Depuis lors, vous avez évoqué en commission, ici au Parlement de Wallonie, comment Fédération Wallonie-Bruxelles, la logique d'une compensation lorsqu'on regarde globalement Wallonie et Fédération Wallonie-Bruxelles – c'est un élément que j'ai retenu – et également probablement la prise en compte de postes qui ne sont pas pourvus. C'est aussi un élément que j'ai retenu, mais qui semble à éclaircir. Bref, la situation reste floue et incertaine. J'en viens directement avec les questions qui faisaient l'objet de cette question écrite.

Quel est l'impact budgétaire brut prévu pour l'augmentation des rémunérations fixes décidée par le Gouvernement wallon pour les *tops managers*, hors compensation éventuelle par réduction du nombre d'emplois de mandataires ? Avant que l'on ne fasse une compensation, à combien sommes-nous ?

Quelles sont les hypothèses derrière les chiffres ? Parce que l'on se rappelle l'opération de dissimulation de la réelle augmentation menée par le Gouvernement et que nous avons démasquée, tenant compte du chipotage sur l'ancienneté. Pour rappel, l'ancienneté pour les agents qui viennent en dehors de la fonction publique est plafonnée à six ans aujourd'hui, sauf exception, pour l'ensemble des agents.

Quel est l'impact budgétaire prévu pour l'établissement d'une rémunération variable prévu par le Gouvernement ? Cette question a été formulée avant le moment où le Gouvernement a décidé de reporter de quelques années cette partie de son projet. Pouvez-vous préciser les hypothèses prises en compte, en termes de proportion d'octrois de cette rémunération variable ? Dès lors qu'elle est variable, combien compte-t-on, en proportion, lorsqu'on fait des estimations budgétaires ?

Y a-t-il d'autres impacts budgétaires à prendre en compte liés au contenu de la réforme, comme des éléments complémentaires à la rémunération, des frais, et cetera ? Si oui, quel est leur impact estimé ?

Depuis lors, nous avons pu prendre connaissance de la note au Gouvernement qui évoque un surcoût par rapport à la trajectoire budgétaire de 4 389 000 euros en 2027, de 4 451 000 euros en 2028, de 4 515 000 euros en 2029 et de plus de 4 579 000 euros en 2030. On est là avec des sommes significatives, qui apparaissent dans un document dans le Gouvernement. Comment expliquer cela ?

L'hypothèse que je formule, c'est que le calcul est peut-être fait en prenant en compte, dans la compensation, des postes qui existent au cadre, mais qui ne sont pas pourvus. Ce qui amènerait un nouvel élément du prix complémentaire à tous ceux qui existent déjà et qui émaillent ce dossier.

Je vous remercie pour les éclaircissements que vous ne manquerez pas de donner aujourd'hui.

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Monsieur le Député, comme j'ai déjà eu l'occasion de l'indiquer, l'impact budgétaire de la réforme des emplois de haut manager doit être apprécié dans sa globalité. La réforme concerne l'ensemble de son périmètre d'application, tant en Région wallonne qu'en Fédération Wallonie-Bruxelles. La neutralité budgétaire poursuivie doit dès lors s'apprécier globalement, en prenant en considération le SPW et les UAP en Région wallonne, ainsi que le ministère de la Fédération Wallonie-Bruxelles et les OIP.

S'agissant tout d'abord de l'augmentation des rémunérations fixes, son impact budgétaire brut, calculé à cadre complet et indépendamment de la rationalisation du nombre d'emplois de haut manager, est estimé à 1,3 million d'euros. Ce montant doit toutefois être mis en perspective avec les travaux de rationalisation des structures et du nombre d'emplois de haut manager, menés parallèlement à la réforme, et être considéré avec prudence.

À titre d'illustration, les simulations budgétaires actuellement disponibles pour le SPW reposent sur une hypothèse de travail de 53 emplois, contre 63 emplois dans le cadre organique théorique actuel. Sur cette base, le coût projeté s'établit à 10,337 millions d'euros en 2027, revalorisation des rémunérations fixes comprises, contre 10,975 millions d'euros dans l'hypothèse où le cadre organique actuel serait intégralement pourvu, soit un différentiel d'environ 638 000 euros. Cette simulation ne préjuge pas du nombre d'emplois qui sera finalement retenu, les travaux relatifs à la rationalisation du cadre du SPW étant toujours en cours. Elle permet néanmoins de mettre en perspective l'impact de la revalorisation des rémunérations avec celui de la rationalisation envisagée.

S'agissant de la rémunération variable, celle-ci est plafonnée à 20 % de la rémunération annuelle brute. Son octroi n'est pas automatique. Il dépendra de l'évaluation et du degré d'atteinte des objectifs fixés. Son entrée en vigueur est désormais prévue à partir de 2030, sauf décision contraire du Gouvernement. Elle n'entraîne dès lors aucun impact budgétaire sur la période 2027-2029. Aucune hypothèse relative à une proportion d'octroi de cette rémunération variable ne doit donc être intégrée dans les projections budgétaires portant sur cette période. À partir de 2030, son impact dépendra du nombre de hauts managers concernés, des résultats de leur évaluation et du niveau de rémunération variable effectivement octroyé.

Enfin, s'agissant des éléments complémentaires à la rémunération, la réforme prévoit un budget mobilité. Les montants retenus à ce titre respectent ceux prévus

par la *car policy* applicable. Ces différents éléments doivent être appréciés conjointement et mis en regard des effets de la rationalisation des structures et du nombre d'emplois de hauts managers. La neutralité budgétaire de la réforme s'apprécie ainsi globalement sur l'ensemble de son périmètre en Région wallonne et en Fédération Wallonie-Bruxelles, en tenant compte des cadres qui seront finalement arrêtés.

Mme la Présidente. – La parole est à M. Hazée.

M. Stéphane Hazée (Ecolo). – Je remercie la ministre. C'est toujours une politesse de le faire pour les éléments qu'elle formule ici. Je les relirai à tête reposée, parce que cela mérite la plus grande précision. Cela semble néanmoins confirmer, sous réserve de relecture, l'hypothèse que je formulais, à savoir que la compensation évoquée est calculée par rapport à des postes qui aujourd'hui ne sont pas occupés et qui, dès lors, ne donnent pas lieu à rémunération. Ce serait donc alors, à nouveau, une certaine forme de vue de l'esprit.

Par ailleurs – mais ce sont des éléments que j'ai ajoutés à la question, parce que l'information est postérieure à la question écrite, qui date d'il y a quelque temps –, je reviendrai ultérieurement par rapport à ces montants extrêmement importants, d'un tout autre ordre de grandeur, en tout cas, qui figurent dans la note au Gouvernement, et qui s'élèvent à 4,5 millions, selon les années. Ces éléments méritent encore un certain approfondissement avant d'aboutir – enfin, je l'espère – à une transparence complète sur ce dossier.

**Question orale
de Mme Éliane Tillieux
à Mme Jacqueline Galant, Ministre de la
Fonction publique, de la Simplification
administrative et des Infrastructures sportives,
sur « le suivi de l'examen du quatorzième
rapport annuel du médiateur »**

**Question orale
de Mme Éliane Tillieux
à Mme Jacqueline Galant, Ministre de la
Fonction publique, de la Simplification
administrative et des Infrastructures sportives,
sur « la procédure intégrée de gestion des
réclamations au sein du Service public de
Wallonie (SPW) »**

**Question orale
de Mme Éliane Tillieux
à Mme Jacqueline Galant, Ministre de la
Fonction publique, de la Simplification
administrative et des Infrastructures sportives,
sur « les tableaux de bord de suivi des
recommandations du médiateur »**

Mme la Présidente. – L'ordre du jour appelle les questions orales à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, de :

- Mme Tillieux, sur « le suivi de l'examen du quatorzième rapport annuel du médiateur » ;
- Mme Tillieux, sur « la procédure intégrée de gestion des réclamations au sein du Service public de Wallonie (SPW) » ;
- Mme Tillieux, sur « les tableaux de bord de suivi des recommandations du médiateur ».

La parole est à Mme Tillieux pour poser ses questions.

Mme Éliane Tillieux (PS). – Madame la Ministre, lors de l'examen du rapport annuel du médiateur en commission, le 13 juillet dernier, le rôle des réclamations comme outil de gouvernance et d'amélioration continue a été mis en avant. À cette occasion, le médiateur a évoqué le concept « d'administration apprenante qui progresse par ses erreurs », illustrant la nécessité pour les services publics de ne pas seulement résoudre des dossiers individuels, mais surtout de tirer les enseignements collectifs des dysfonctionnements constatés. La transformation des retours d'expérience et des plaintes en évolution administrative concrète est en effet essentielle pour renforcer la confiance des usagers.

Dès lors, quelle stratégie développez-vous pour promouvoir cette culture d'administration apprenante au sein du SPW et des OIP ? Un système structuré de partage des bonnes pratiques et de retours d'expérience

est-il organisé entre les différentes directions générales, sur la base des cas traités par le médiateur et par la première ligne de traitement des plaintes ? Comment ces enseignements sont-ils intégrés dans la formation des agents et le pilotage du management de la fonction publique wallonne ?

Lors de notre séance de commission consacrée à l'examen du rapport annuel du médiateur, nous avons aussi abordé le fonctionnement de la procédure intégrée de gestion des réclamations. Le mécanisme repose sur une complémentarité entre une première ligne, c'est-à-dire la gestion interne des plaintes directement dans l'administration du Service public de Wallonie, et la deuxième ligne qui est assurée par M. le Médiateur.

À cette occasion, j'ai demandé si un rapport consolidé des plaintes de première ligne du SPW avait été transmis au médiateur ainsi qu'au Gouvernement et si ce document pouvait être communiqué au Parlement. Une telle transmission est indispensable pour garantir la transparence sur le volume des plaintes enregistrées, le délai de réponse, les motifs récurrents d'insatisfaction et les corrections apportées par l'administration.

Vous n'avez toutefois pas eu l'opportunité de me répondre sur ce point précis. C'est la raison pour laquelle je reviens à nouveau vers vous. Un rapport consolidé annuel sur les plaintes de première ligne du SPW est-il bien établi ? Est-il transmis au médiateur ? Est-il transmis au Gouvernement ? Êtes-vous en mesure de communiquer ce rapport aux membres du Parlement pour nourrir notre contrôle démocratique ? Quels sont les principaux enseignements et indicateurs clés qui en ressortent quant aux délais de traitement et surtout à l'efficacité interne du traitement des réclamations ?

L'importance des tableaux de bord de suivi a été mise en avant par M. le Médiateur en tant qu'outil de pilotage et de contrôle parlementaire. À cette occasion, je vous ai demandé si vous pouviez transmettre au Parlement le tableau de bord de suivi des recommandations du médiateur pour les services qui relèvent de vos compétences. Vous m'avez répondu que le tableau devait au préalable être finalisé et consolidé avec l'ensemble des membres du Gouvernement wallon avant qu'il puisse être transmis aux députés. Je vous ai alors interrogée sur le délai nécessaire à cette finalisation.

Depuis lors, deux mois se sont écoulés et, alors que la rentrée parlementaire est effective, ce suivi reste indispensable pour évaluer la concrétisation des recommandations et l'amélioration continue de nos services publics. Le travail de consolidation du tableau de bord entre les différents membres du Gouvernement est-il achevé ou est-il toujours en cours ? Êtes-vous en mesure de le communiquer au Parlement ? Ce document détaille-t-il, pour chaque recommandation, l'état d'avancement des démarches – ce qui est réalisé, en

cours, reporté ou abandonné – ainsi que les raisons des éventuels blocages ?

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Madame la Députée, la notion d'administration apprenante évoquée par le médiateur rejoint la démarche d'amélioration continue poursuivie au sein du SPW. L'enjeu est de ne pas considérer une plainte ou une difficulté comme un cas isolé, mais de pouvoir identifier les difficultés récurrentes pour en comprendre les causes et en tirer les enseignements utiles afin d'améliorer le fonctionnement de l'administration et le service rendu aux usagers.

Depuis 2019, le SPW dispose d'un processus commun de gestion des réclamations de première ligne appliqué dans l'ensemble de ses directions générales. Celui-ci prévoit l'enregistrement et l'examen de la recevabilité de la plainte, son orientation vers le service compétent, son traitement, l'envoi d'une réponse circonstanciée à l'utilisateur ainsi qu'un travail de rapportage et d'amélioration continue.

Ce dispositif est complété par l'intervention du médiateur dans le cadre de ses compétences propres. Ses analyses et recommandations contribuent également aux réflexions et aux ajustements des processus internes.

Un système structuré de partage des bonnes pratiques et de retours d'expérience existe entre les différentes directions générales du SPW. Il permet de capitaliser sur les difficultés rencontrées, d'identifier celles qui présentent un caractère récurrent, de partager les enseignements qui peuvent en être tirés et de suivre les mesures correctrices décidées.

Cette démarche ne repose toutefois pas uniquement sur les plaintes formellement introduites. Tous les usagers rencontrant une difficulté n'introduisent pas nécessairement une réclamation. L'approche développée en matière d'expérience usager permet dès lors de prendre également en considération les enquêtes, les ateliers, les panels et les données relatives au parcours administratif.

Le référentiel usager fournit désormais un cadre commun à ce travail. Cette approche s'inscrit également dans le choc de simplification qui vise plus largement à faire évoluer les pratiques administratives et, lorsque cela s'avère nécessaire, à réexaminer les démarches et les parcours des usagers.

Les enseignements issus de ces différents retours ont également vocation à nourrir les pratiques professionnelles, notamment en matière d'écoute des usagers, de rédaction claire, de gestion par processus, de maîtrise des risques et de principe de confiance. Ils

peuvent également contribuer au pilotage managérial en permettant de porter l'attention non seulement sur le nombre de plaintes et les délais de réponse, mais également sur les difficultés récurrentes et les actions correctrices mises en œuvre.

S'agissant plus spécifiquement du rapportage des plaintes en première ligne, un rapport consolidé annuel est élaboré dans le cadre de la gestion interne du SPW. Il reprend les données communiquées par les différentes directions générales et présente notamment le nombre de plaintes reçues, leur recevabilité, les plaintes ne relevant pas de compétence du SPW, les transferts entre directions générales, les principales thématiques d'insatisfaction ainsi que les constats et pistes d'amélioration communiqués par les services.

En 2025, 423 plaintes ont été comptabilisées dans le dispositif de première ligne du SPW, dont 64 % correspondaient à des plaintes recevables relevant de ses compétences. À titre de comparaison, 516 plaintes avaient été enregistrées en 2024, dont 372 recevables. Cette diminution du nombre de plaintes enregistrées doit toutefois être interprétée avec prudence. Certaines plaintes sont en effet adressées directement aux services et ne sont pas toujours enregistrées dans le circuit central. Il ne serait dès lors pas correct d'en déduire automatiquement une évolution au niveau de la satisfaction des usagers.

Les données disponibles montrent également qu'un certain nombre de plaintes sont mal orientées ou concernent des matières ne relevant pas des compétences du SPW. L'amélioration de la lisibilité des canaux d'entrée et l'orientation des usagers constitue dès lors un point d'attention.

Les motifs d'insatisfaction varient selon les matières et peuvent notamment concerner les délais de traitement, les traitements des dossiers et l'application des procédures, la qualité du service rendu, l'attitude des agents, l'accès à l'information, les primes, l'état et la sécurité des voiries ou encore l'accessibilité de certaines démarches numériques.

Le processus commun fixe comme standard l'envoi d'un accusé de réception dans les 10 jours et d'une réponse dans un délai maximal de 40 jours. Le rapport 2024 concluait que les gestionnaires avaient traité les plaintes de manière satisfaisante et dans les délais impartis. Il relevait également une bonne relation de travail avec le médiateur.

Le rapport consolidé 2025 ne permet toutefois pas encore d'établir, de manière transversale, pour l'ensemble du SPW, le délai moyen ou médian de traitement ni la proportion exacte des plaintes clôturées dans le délai de 40 jours. Cet élément pourra utilement être pris en considération dans la poursuite de l'amélioration du rapportage.

Le rapport consolidé est actuellement présenté annuellement aux instances internes compétentes du SPW. Sa transmission au Parlement n'est, à ce stade, ni systématique ni formalisée. Cela étant, la question d'une diffusion plus large des principaux enseignements et indicateurs issus de ce rapport mérite d'être examinée avec l'administration afin d'en apprécier les modalités et de déterminer les informations qui pourraient utilement être partagées.

Enfin, concernant le suivi des recommandations du médiateur, le tableau de bord de suivi des recommandations issues des audits internes et externes, incluant les recommandations transversales du médiateur, est transmis annuellement au Gouvernement. À ce stade, ces tableaux de bord se déclinent selon les différentes compétences fonctionnelles compte tenu de leurs spécificités. Le travail de consolidation s'opère donc au niveau de chacune de ces compétences, comme c'est également le cas lorsque le médiateur rencontre les différentes commissions parlementaires dans le cadre de la remise de son rapport annuel.

Plus largement, le travail se poursuit afin d'améliorer progressivement les dispositifs existants, tant en matière de suivi et de rapportage que de partage des enseignements issus des réclamations et des recommandations du médiateur. L'objectif reste de permettre à l'administration d'identifier les difficultés récurrentes, d'en tirer les enseignements utiles et, lorsque cela s'avère nécessaire, d'adapter ses pratiques. C'est dans cette dynamique d'amélioration continue que s'inscrit la démarche d'administration apprenante évoquée par le médiateur.

Mme la Présidente. – La parole est à Mme Tillieux.

Mme Éliane Tillieux (PS). – Qu'il s'agisse de la transmission des tableaux de bord, de la communication du rapport des plaintes de première ligne ou de la promotion d'une administration apprenante, l'enjeu central est toujours le même : doter le Parlement d'outils de contrôle objectifs pour évaluer l'amélioration réelle des services publics. Pour qu'une administration soit réellement apprenante, elle doit analyser de manière transversale les plaintes internes, c'est-à-dire de la première ligne, et les concilier avec les avis de la deuxième ligne, c'est-à-dire du médiateur. Cela nécessite aussi une communication de ces bilans consolidés vers le Parlement.

Le médiateur lui-même nous invitait à ne pas nous limiter à un inventaire des plaintes. Ce qui importe, c'est l'analyse qui en est faite de manière transversale et surtout les enseignements systémiques qui en sont tirés pour éviter que les difficultés se reproduisent indéfiniment. Le médiateur relevait que « l'administration ne parle pas à l'administration » : les bonnes pratiques existent, encore faut-il qu'elles soient identifiées, partagées et même généralisées quand cela se justifie.

Le droit à l'erreur, comme l'évoquait M. le Médiateur, et l'apprentissage continu ne peuvent pas rester des concepts théoriques, surtout dans un contexte où ils sont confrontés à une réduction d'effectifs pas toujours concertée, une numérisation parfois précipitée, où l'on manque de formation des agents. Il y a dès lors, au travers de ces enseignements, des efforts encore à poursuivre pour tenter d'améliorer la qualité du service à nos citoyennes et citoyens.

**Question orale
de Mme Éliane Tillieux
à Mme Jacqueline Galant, Ministre de la
Fonction publique, de la Simplification
administrative et des Infrastructures sportives,
sur « le suivi de la cybersécurité des services
publics wallons »**

Mme la Présidente. – L'ordre du jour appelle la question orale de Mme Tillieux à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « le suivi de la cybersécurité des services publics wallons ».

La parole est à Mme Tillieux pour poser sa question.

Mme Éliane Tillieux (PS). – C'est un peu bête, j'aurais dû poser ma question dans le cadre des auditions tout à l'heure, mais je vais la poser maintenant.

Madame la Ministre, un article de presse consacré à un rapport de la Cour des comptes fait état de fragilité persistante dans la préparation de plusieurs administrations publiques face aux cyberattaques, notamment en matière de plan de reprise, de tests réguliers ou de moyens consacrés à la cybersécurité. Même si le rapport porte sur des entités fédérales, ces constats font écho à l'attaque subie par le Service public de Wallonie, le 17 avril 2025, qui avait perturbé plusieurs services essentiels.

Lors de la Commission du 14 septembre, vous avez déjà apporté plusieurs informations. Suite à l'article de presse, pourriez-vous préciser si l'évaluation de la maturité en cours porte également sur les organismes publics wallons qui relèvent de la compétence du Gouvernement et concernés par les exigences de cybersécurité applicables ?

Les principales lacunes et vulnérabilités prioritaires ont-elles déjà été identifiées ? Combien de services du SPW disposent actuellement d'un plan de continuité et d'un plan de reprise à jour ayant fait l'objet d'un test ? Combien d'exercices de crise ont été organisés depuis l'attaque de 2025 ? Quelles mesures correctrices ont été décidées à la suite de ces exercices ?

Quels moyens budgétaires et humains sont actuellement consacrés à la cybersécurité de notre administration ? On l'a déjà évoqué un peu tout à l'heure, mais peut-être avez-vous des informations complémentaires. Ces moyens sont-ils considérés comme suffisants pour mettre en œuvre la stratégie 2025-2029 et la future feuille de route ? Quels moyens supplémentaires – nous n'avons pas encore évoqué ce sujet – devront être prévus à partir de 2027 ? La feuille de route annoncée pour le début de l'année 2027 comprendra-t-elle des échéances précises, la désignation de responsabilités de chaque entité, des indicateurs de suivi et un mécanisme de contrôle régulier ? Un rapport d'avancement sera-t-il transmis au Parlement wallon ?

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Madame la Députée, vous m'interrogez sur le suivi de la cybersécurité au sein des services publics wallons à la lumière des enseignements tirés de la cyberattaque du 17 avril 2025 – nous en avons parlé toute l'après-midi – et de l'évaluation de la maturité actuellement menée au sein du SPW.

Je souhaite d'abord préciser le périmètre de cette évaluation qui correspond au périmètre de mes compétences. Le marché lancé à la fin de l'année 2025 concerne le SPW, qui constitue la seule entité relevant des exigences de la directive NIS 2. Cette évaluation ne couvre donc pas les UAP, qui doivent organiser leur propre démarche d'évaluation. Le SPW n'a, par ailleurs, ni la mission de superviser ces évaluations ni, à ce stade, une vue consolidée des démarches menées par chacune de ces unités. L'évaluation en cours, qui s'inscrit dans la stratégie de cybersécurité établie par le SPW et validée par le Gouvernement en juillet 2025, doit permettre de disposer, d'ici la fin de l'année, d'une vision consolidée des principaux écarts de maturité et des mesures à traiter en priorité dans les différentes directions du SPW.

Les travaux sont donc toujours en cours. Je ne dispose pas encore de tous les éléments demandés. Cela étant, vous comprendrez sans doute qu'il ne serait pas responsable de rendre publiques des informations détaillées sur la nature, la localisation ou la criticité de vulnérabilités susceptibles d'être exploitées à des fins malveillantes. Les informations qui pourront être communiquées le seront dès lors de manière agrégée, en portant sur les grandes catégories de risques, l'état d'avancement général et les actions correctrices engagées.

En ce qui concerne les plans de continuité et de reprise, nous sortons de la compétence digitale en tant que telle, puisqu'il s'agit de la gestion de crise en général. À ce jour, le SPW est toujours occupé à la réalisation d'un inventaire consolidé permettant

d'indiquer combien de services disposent actuellement de plans à jour et effectivement testés. Plusieurs directions du SPW ont néanmoins déjà élaboré et intégré des plans de continuité dans leurs pratiques. L'évaluation de maturité en cours doit précisément nous permettre d'établir une situation consolidée sur ce volet, y compris sur le niveau d'actualisation et de test des dispositifs.

Depuis la cyberattaque de 2025, deux exercices de crise cyber ont été organisés. Ils ont notamment mis en évidence la nécessité d'améliorer les canaux de communication et les modalités de partage de l'information en situation de crise. Ces exercices seront désormais organisés chaque année afin de tester les dispositifs, de vérifier l'application des procédures et d'alimenter une logique d'amélioration continue. Parallèlement, le SPW renforce progressivement la prévention, la détection, la réponse aux incidents et la résilience de ses systèmes d'information.

S'agissant des moyens budgétaires consacrés à la cybersécurité, les crédits d'engagement initiaux inscrits en 2026 dans le périmètre du SPW Digital s'élèvent à 11,172 millions d'euros. Ils financent la coordination du programme de sécurité du SPW. À ceux-ci s'ajoutent 3,8 millions d'euros consacrés à la sécurité des équipements industriels du SPW Mobilité et Infrastructures, ainsi que 1,5 million d'euros provenant des différentes entités du SPW pour leur contribution au marché d'évaluation de maturité. Le montant consolidé consacré en 2026 aux activités de sécurité et d'information du SPW est ainsi évalué à environ 16,5 millions d'euros.

Concernant les moyens humains, il n'existe pas encore d'indicateur consolidé permettant d'isoler précisément l'ensemble des personnes qui interviennent exclusivement ou partiellement dans le domaine de la cybersécurité. Ces missions mobilisent à la fois des équipes spécialisées, des fonctions transversales, des responsables métiers, des équipes techniques et – cela s'avère nécessaire – des prestataires disposant d'une expertise spécifique.

Les moyens actuels permettent de mettre en œuvre des actions identifiées comme prioritaires, notamment suite aux recommandations des experts qui nous ont accompagnés en 2025, en tenant compte également de la capacité de l'administration à absorber ces transformations. Il serait toutefois prématuré d'affirmer qu'ils suffiront pour couvrir l'ensemble de la stratégie 2025-2029 et la future feuille de route. C'est précisément l'évaluation de maturité qui permettra de définir la trajectoire pluriannuelle, de hiérarchiser les priorités et d'objectiver les moyens humains et financiers nécessaires pour atteindre le niveau d'ambition retenu.

Pour 2027, comme je l'ai dit tantôt, les demandes actuellement formulées portent notamment sur

14,3 millions d'euros pour le SPW Digital ; 4,7 millions d'euros pour le SPW Mobilité et Infrastructures ; et un reliquat de 150 000 euros lié à l'évaluation de la maturité pour les autres métiers. Ces montants demeurent toutefois des demandes budgétaires et devront être confirmés dans le cadre des arbitrages et des négociations budgétaires.

La feuille de route attendue au début de l'année 2027 ne se limitera pas à dresser un constat. Elle devra transformer les résultats de l'évaluation en une trajectoire structurée de mise en conformité et de renforcement de résilience. Elle intégrera les écarts identifiés, la responsabilité des différentes parties prenantes et les actions prioritaires à un calendrier, des jalons de mise en œuvre ainsi que les modalités de gouvernance nécessaires au suivi dans la durée. Son pilotage devra également s'appuyer sur des indicateurs, un suivi des actions correctrices, une gestion structurée des risques et des revues régulières permettant de mesurer le progrès et, si nécessaire, d'adapter les priorités.

Enfin, le Gouvernement entend assurer un suivi structuré, transparent de cette démarche. Le Parlement wallon sera informé de son avancement dans le cadre des mécanismes habituels de contrôle démocratique. Les modalités précises de ce rapportage seront arrêtées après la consolidation des résultats de l'évaluation et la validation de la feuille de route.

Cet exercice de transparence devra naturellement être concilié avec l'obligation de ne pas rendre publiques des informations susceptibles de compromettre la sécurité des systèmes concernés.

Mme la Présidente. – La parole est à Mme Tillieux.

Mme Éliane Tillieux (PS). – Madame la Ministre, il va de soi que les informations que nous sollicitons ne doivent pas mettre en danger ou en difficulté la sécurité ; ce serait contre-productif. On en a déjà largement parlé.

Néanmoins, les parlementaires doivent aussi exercer leur rôle de contrôle. Donc, s'il le faut, pourquoi pas une commission à huis clos. Je n'ai pas de demande actuellement, mais c'est toujours quelque chose que nous pourrions envisager lorsque vous aurez les résultats de l'évaluation de la maturité et que vous mettrez en place cette fameuse feuille de route qui est attendue pour 2027.

Je réitère la nécessité des moyens suffisants pour mettre en œuvre toute cette dynamique avec un budget. Vous avez rappelé les chiffres de la demande ; j'espère qu'ils pourront être retenus dans le cadre du conclave budgétaire et des arbitrages qui auront lieu.

Je retiens surtout que les démarches sont engagées en termes de sécurité – on en a largement parlé cet après-midi – et que des éléments essentiels restent

encore en construction, notamment l'évaluation de la maturité, mais aussi la généralisation des plans de continuité et de reprise et la feuille de route opérationnelle qui devra venir au terme de tout cela. On continue à suivre attentivement ce dossier.

Question orale
de M. Thierry Witsel
à Mme Jacqueline Galant, Ministre de la
Fonction publique, de la Simplification
administrative et des Infrastructures sportives,
sur « l'impact de la sécheresse sur les terrains
de football wallons »

Mme la Présidente. – L'ordre du jour appelle la question orale de M. Witsel à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « l'impact de la sécheresse sur les terrains de football wallons ».

La parole est à M. Witsel pour poser sa question.

M. Thierry Witsel (PS). – Madame la Ministre, la Wallonie a connu cet été une nouvelle période de sécheresse et de fortes chaleurs qui ont affecté notamment les espaces verts et les infrastructures sportives.

Les terrains de football en gazon naturel sont particulièrement exposés à ces conditions climatiques. Le manque de précipitations et les températures élevées peuvent entraîner un dessèchement important des pelouses, une dégradation de la qualité des surfaces de jeu et, dans certains cas, des dégâts nécessitant des travaux de remise en état ou des dépenses supplémentaires d'entretien et d'arrosage.

Cette situation intervient alors que les pouvoirs publics sont par ailleurs invités à limiter la consommation d'eau, notamment pour l'arrosage des terrains sportifs. Elle peut donc représenter une difficulté supplémentaire pour les communes et les gestionnaires d'infrastructures sportives, qui doivent préserver des terrains parfois récemment aménagés ou rénovés.

Votre administration dispose-t-elle d'un état des lieux des dégâts occasionnés par la sécheresse actuelle sur les terrains de football wallons en gazon naturel ? Des communes, régions autonomes ou gestionnaires d'infrastructures sportives ont-ils informé votre administration de dégradations importantes de leurs terrains liées à la sécheresse ?

Certains pouvoirs locaux ont-ils sollicité auprès de votre cabinet ou de votre administration une aide financière ou un soutien de la Région wallonne afin de faire face aux conséquences de cette sécheresse ? Des aides ou mécanismes de soutien spécifiques peuvent-ils

être mobilisés lorsque des infrastructures sportives récemment subsidiées par la Région subissent des dégâts liés à des conditions climatiques exceptionnelles ?

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Monsieur le Député, je comprends tout à fait la question que vous soulevez. Nous avons constaté cet été que certaines pelouses avaient fortement souffert des périodes de chaleur et du manque de précipitations, avec parfois un dessèchement des surfaces.

Dans certains cas, de tels épisodes peuvent naturellement entraîner des dégradations plus importantes et nécessiter des interventions spécifiques.

À ce stade, cependant, aucune commune, régie communale autonome ou gestionnaire d'infrastructures sportives n'a signalé à Infraspports de dégradation importante des terrains imputables à la sécheresse, ni sollicité d'intervention particulière à ce titre.

S'agissant d'un éventuel mécanisme de soutien spécifique, aucun dispositif particulier n'a été identifié à ce stade dans le cadre d'Infraspports pour répondre à ce type de situation. Je rappelle que l'entretien des infrastructures sportives relève de la responsabilité de leur gestionnaire, y compris lorsqu'elles ont bénéficié d'un subventionnement régional.

Si des cas concrets devaient être toutefois portés à la connaissance de mon administration, ils pourraient naturellement être examinés au regard du cadre réglementaire existant et des dispositifs éventuellement mobilisables.

Plus largement, les questions liées à la gestion de l'eau et à l'adaptation des infrastructures sportives aux épisodes climatiques extrêmes doivent être prises en considération dans nos réflexions, notamment dans le cadre de l'évolution en cours du décret Infraspports.

Mme la Présidente. – La parole est à M. Witsel.

M. Thierry Witsel (PS). – Je remercie Mme la Ministre pour ses éléments de réponse. Il faut soutenir les clubs de sport – de foot en l'occurrence – qui, du jour au lendemain, suite à la sécheresse, perdent leur terrain, leur pelouse, pour que les jeunes puissent continuer à s'entraîner. Quand je suis rentré de vacances, la pelouse de chez moi était toute séchée. C'est important pour continuer à s'entraîner dans de bonnes conditions.

Vous l'avez dit, il n'y a peut-être pas eu de demande spécifique, mais je vois que vous restez ouverte concernant la situation. Il faut, dans tous les cas, faire en

sorte que les clubs puissent être soutenus par votre administration à l'avenir et par les subsides ou les soutiens que vous pouvez amener.

Question orale
de M. Thierry Witsel
à Mme Jacqueline Galant, Ministre de la
Fonction publique, de la Simplification
administrative et des Infrastructures sportives,
sur « l'avenir de l'infrastructure de
l'hippodrome de Wallonie après le
désengagement régional »

Mme la Présidente. – L'ordre du jour appelle la question orale de M. Witsel à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « l'avenir de l'infrastructure de l'hippodrome de Wallonie après le désengagement régional ».

La parole est à M. Witsel pour poser sa question.

M. Thierry Witsel (PS). – Madame la Ministre, vous rappeliez vous-même en décembre 2024 que ce dossier relevait à la fois de l'Économie et d'Infrasports. C'est également dans le cadre de vos compétences que le Gouvernement a supprimé, dès 2025, la subvention annuelle de 950 000 euros accordée à l'hippodrome.

Près de deux ans plus tard, force est de constater que le désengagement public a précédé la mise en place d'une solution pérenne : la reprise n'est toujours pas finalisée, et le mécanisme de retour sur filière n'existe toujours pas.

La dernière actualité cite un investisseur privé français qui se nomme Xavier Rouet, actif dans la retransmission des courses sur les différents hippodromes belges et néerlandais. Toutefois, il a émis les conditions d'une réforme du financement de la filière hippique belge, notamment permettant qu'une partie des mises réalisées sur les courses hippiques bénéficient directement à la filière belge, sujet que M. Achille Cassart, le CEO de l'hippodrome, a déjà proposé.

Avec le recul, estimez-vous que supprimer intégralement le financement, avant qu'un modèle alternatif soit opérationnel, constituait la bonne séquence ? Quel suivi votre cabinet assure-t-il aujourd'hui, avec votre collègue en charge de l'Économie, concernant l'avenir sportif de cette infrastructure ? Avez-vous évalué les conséquences de la suppression des 950 000 euros sur son activité, son entretien et ses investissements ? Quelles garanties exigez-vous afin qu'une éventuelle privatisation ne conduise pas, demain, à une réduction progressive de la vocation sportive et hippique du site ?

Au vu de l'actualité récente, je souhaiterais émettre deux ou trois questions supplémentaires. Quelles garanties précises accompagnez-vous à cette cession, afin d'assurer le maintien durable de la vocation hippique et sportive du site ? Une obligation de maintien des pistes et des principales structures sportives est-elle prévue dans les conditions de cession ? Une durée minimale d'affectation sportive sera-t-elle imposée au repreneur ? Des clauses sont-elles prévues pour éviter que, une fois la cession réalisée, une partie du site ou des infrastructures puisse progressivement être réaffectée, cédée ou démantelée au détriment de l'activité hippique ? Quelles garanties avez-vous enfin obtenues concernant la poursuite des activités, des écoles, des formations et plus largement de l'ensemble des utilisateurs sportifs du site ?

Enfin, Madame la Ministre, la Région peut décider de ne plus être actionnaire, mais elle ne peut pas se désintéresser du devenir d'une infrastructure sportive qu'elle a contribué à créer et à développer au fil des années précédentes.

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Monsieur le Député, je voudrais tout d'abord rappeler précisément le cadre de ce dossier. Le Gouvernement a en effet fait le choix de mettre fin, à partir de 2025, aux subventions régionales de fonctionnement de l'hippodrome de Wallonie. Parallèlement à cette décision, la Région a engagé un processus de cession de sa participation dans l'Hippodrome de Wallonie. Ce processus est suivi par Wallonie Entreprendre dans le cadre de la mission qui lui était confiée, en concertation avec le ministre de l'Économie.

Des démarches ont été menées en vue d'identifier un investisseur ou un repreneur, et le dossier a connu des avancées récentes, comme cela a été relayé dans la presse. Des discussions doivent désormais avoir lieu au sein du Gouvernement sur les éventuelles conditions d'une opération de cession. Je continue à suivre de près ce dossier et reste persuadée qu'une issue favorable pourrait être trouvée dans les prochaines semaines.

Mme la Présidente. – La parole est à M. Witsel.

M. Thierry Witsel (PS). – Madame la Ministre, je vous remercie pour ces informations. Je n'ai pas reçu la réponse à mes questions. Je rappelle tout de même que l'hippodrome, ce sont plus de 20 hectares, ce sont des pistes, des manèges, des écoles, des formations. C'est toute une filière qui est présente à cet endroit.

Je rappelle que 950 000 euros de financement ont été supprimés. C'est probablement un choix qui reste politique. Cela fait maintenant deux ans à minima que l'on attend des réponses concrètes sur l'avenir de

l'hippodrome de Wallonie, même s'il y a un probable repreneur et que ce sera discuté au sein du Gouvernement, il y a des écoles, des formations et des manèges qui sont présents. Toute cette filière attend des réponses concrètes pour savoir ce qu'ils vont devenir dans les semaines et les mois à venir. Mon collègue interrogera votre collègue, M. Pierre-Yves Jeholet, sur le suivi de l'hippodrome de Wallonie.

**Question orale
de M. Vincent Maillen
à Mme Jacqueline Galant, Ministre de la
Fonction publique, de la Simplification
administrative et des Infrastructures sportives,
sur « l'homologation des terrains synthétiques
sans remplissage et la stratégie
d'accompagnement »**

Mme la Présidente. – L'ordre du jour appelle la question orale de M. Maillen à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « l'homologation des terrains synthétiques sans remplissage et la stratégie d'accompagnement ».

La parole est à M. Maillen pour poser sa question.

M. Vincent Maillen (MR). – Madame la Ministre, dans le cadre des travaux de notre Commission, nous avons eu l'opportunité d'effectuer des visites de terrains sportifs synthétiques sans aucun remplissage.

Cette démarche s'inscrit au cœur d'un enjeu majeur pour nos infrastructures. L'Union européenne a en effet acté l'interdiction de la mise sur le marché des microplastiques d'ici octobre 2031. Cela vise directement les granulés de caoutchouc recyclé utilisés dans la majorité de nos terrains synthétiques, reconnus comme une source importante de pollution microplastique.

Pour anticiper cette échéance – c'est demain –, des alternatives émergent. Nous avons notamment visité le site de Holsbeek, pionnier en la matière, puisqu'il accueille le tout premier terrain synthétique sans remplissage en Belgique en phase de test. Ces technologies *non-infill* représentent une promesse forte : aucun rejet microplastique, un entretien réduit et une empreinte environnementale nettement améliorée, tout en conservant une grande praticité pour les clubs.

Madame la Ministre, nous savons que votre cabinet et vous-mêmes êtes sensibilisés à cette problématique. Aussi, que pensez-vous de cette phase de test à Holsbeek ainsi que les retours d'expérience sur ce type de revêtement ? Quels sont vos échanges avec les fédérations sportives, notamment la FFA – Football Francophone Amateur – quant à l'homologation de ces terrains sans remplissage pour les compétitions

officielles ? Les critères de performance – rebond, absorption des chocs, risque de brûlure, et cetera – satisfont-ils aux exigences des cahiers des charges ?

Enfin, quelle stratégie ou quel cadre normatif comptez-vous déployer pour accompagner nos clubs et communes dans le renouvellement du parc de terrains, afin d'éviter une crise d'infrastructures à l'approche de 2031 ? Comme je l'ai dit, c'est demain.

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Monsieur le Député, la question que vous soulevez est importante parce que nous devons effectivement anticiper les évolutions qui toucheront nos terrains synthétiques dans les prochaines années. Le règlement européen prévoit qu'à partir du 17 octobre 2031, le remplissage granulaire concerné ne pourra plus être mis sur le marché pour être utilisé sur les surfaces sportives synthétiques.

Je précise toutefois qu'il ne s'agit pas d'une obligation de remplacer tous les terrains existants à cette date. Nous disposons encore de plusieurs années pour préparer cette transition et accompagner correctement les communes et les clubs dans leur futur investissement.

Les expériences menées à Holsbeek, mais également sur d'autres installations en Belgique et en Europe, sont particulièrement intéressantes à cet égard. Elles permettent progressivement de disposer de davantage de recul sur ces nouvelles surfaces, notamment en matière de performances, de durabilité, d'entretien, de coût et de confort pour les utilisateurs. Selon les éléments techniques dont dispose mon administration, le cadre FIFA a évolué afin de prendre en compte de nouvelles catégories de surfaces, notamment les systèmes sans remplissage et certains systèmes de remplissage minéral.

S'agissant de l'homologation pour les compétitions officielles, celles-ci relèvent des exigences définies par les fédérations sportives compétentes. Les différents systèmes doivent répondre à des critères techniques en matière de comportement du ballon, d'absorption des chocs, de résistance au glissement ou encore de sécurité des utilisateurs.

Les nouvelles générations de surfaces sans remplissage font aujourd'hui l'objet de retours d'expérience qui doivent permettre d'affiner progressivement le cadre applicable.

Dans ce contexte, nous poursuivons nos échanges avec la Fédération francophone de football. Infrasports estime qu'il est important de disposer d'un positionnement suffisamment clair concernant les terrains sans remplissage et les systèmes de remplissage

minéral, afin d'adapter son cadre normatif et conseiller correctement les porteurs de projet.

Mon administration poursuit sa veille technique et réglementaire sur les différentes solutions disponibles. La documentation technique existante, notamment dans le cadre normatif, ainsi que le guide relatif à la conception, à la construction et à l'entretien des terrains synthétiques devraient également être actualisés dans le courant de l'année 2027 avec l'appui d'un laboratoire agréé. L'objectif n'est pas de privilégier aujourd'hui une technologie plutôt qu'une autre, mais de disposer d'un cadre suffisamment clair et de retours d'expérience suffisamment solides pour conseiller correctement les communes et les clubs et sécuriser les investissements réalisés pour de nombreuses années.

Nous avons encore du temps avant 2031, mais c'est précisément maintenant qu'il faut préparer cette transition.

Mme la Présidente. – La parole est à M. Maillen.

M. Vincent Maillen (MR). – Madame la Ministre, je vous remercie pour cette réponse très claire et complète. C'est un peu ce que j'imaginais, puisque l'on a quand même été bien informés. Je profite d'ailleurs de ma réplique pour remercier les personnes de terrain qui nous ont invités et qui nous ont présenté toutes ces infrastructures différentes, que ce soit à Holsbeek ou à Rixensart.

Je suis un peu un peu étonné que nous n'ayons été qu'en majorité là-bas. Il aurait aussi été intéressant pour l'opposition d'être présente pour voir les...

(Réaction d'un intervenant)

Mais non, je le dis objectivement. Monsieur Witsel, ce n'est pas un problème, je le comprends tout à fait.

Quand je dis l'opposition, c'est toute l'opposition, il n'y a rien de scandaleux.

Mme Éliane Tillieux (PS). – C'est minable. Il y avait des circonstances et je trouve qu'utiliser politiquement cet argument est lamentable.

M. Vincent Maillen (MR). – Je ne vous parle pas. Ai-je la parole ou n'ai-je pas la parole ?

Mme Éliane Tillieux (PS). – Vous nous attaquez !

Mme la Présidente. – C'est M. Maillen qui a la parole.

M. Vincent Maillen (MR). – Vous n'êtes pas toute l'opposition que je sache. Je ne m'attaque pas forcément au PS, il y a aussi le PTB et Ecolo qui n'étaient pas là. Je trouve cela dommage. Évidemment que M. Witsel a des circonstances atténuantes ; je ne parle même pas de cela.

Ce que je veux dire, c'est que l'on est dans une situation où l'on travaille sur ce dossier et tout le monde a besoin d'être là pour ne pas venir dire après qu'il n'a pas compris ou qu'il ne sait pas.

Mme la Présidente. – En effet, M. Witsel était excusé pour son absence. Les autres membres du PS avaient également signalé qu'ils ne seraient pas présents à cette visite.

Question orale

de M. Thierry Witsel

à Mme Jacqueline Galant, Ministre de la
Fonction publique, de la Simplification
administrative et des Infrastructures sportives,
sur « la prévention des noyades par le recours à
l'intelligence artificielle (IA) à la piscine de
Spa »

Mme la Présidente. – L'ordre du jour appelle la question orale de M. Witsel à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « la prévention des noyades par le recours à l'intelligence artificielle (IA) à la piscine de Spa ».

La parole est à M. Witsel pour poser sa question.

M. Thierry Witsel (PS). – C'est juste dommage de le dire au micro.

M. Vincent Maillen (MR). – À un moment donné, je dis les choses, le PS n'est pas toute l'opposition.

M. Thierry Witsel (PS). – Je sais, mais il n'y a que le PS au sein de cette Commission.

M. Vincent Maillen (MR). – On s'est déjà fait alpaguer pour plein de trucs différents. J'ai le droit de dire ce que je pense.

Mme Éliane Tillieux (PS). – Oui, chacun peut s'exprimer comme il le souhaite.

M. Thierry Witsel (PS). – Tout à fait d'accord avec cela, mais il est dommage de l'avoir dit au micro.

Mme la Présidente. – Monsieur Witsel, veuillez poser votre question.

M. Thierry Witsel (PS). – Madame la Ministre, la piscine communale de SPA vient de se doter d'un dispositif particulièrement innovant destiné à renforcer la prévention des noyades. Douze caméras sous-marines permettent de surveiller en permanence l'activité dans le bassin. Lorsqu'une personne reste immobile sous l'eau pendant plusieurs secondes, une intelligence artificielle analyse la situation et déclenche une alerte directement auprès des maîtres-nageurs, notamment via leur montre connectée.

Il s'agit d'un outil qui peut contribuer à améliorer la sécurité des nageurs et à permettre une intervention plus rapide en cas de difficulté. La technologie ne remplace d'ailleurs ni la présence ni la vigilance des maîtres-nageurs, mais vient les épauler dans une situation où chaque seconde peut être déterminante.

Avez-vous connaissance de la mise en place de ce dispositif à la piscine de Spa et avez-vous été informée de ses modalités de fonctionnement ? Des dispositifs similaires de détection des noyades par intelligence artificielle sont-ils actuellement utilisés ou envisagés dans d'autres infrastructures sportives subventionnées par la Wallonie ? Disposez-vous d'une évaluation de l'efficacité de ces technologies en matière de prévention et de détection des noyades ?

Envisagez-vous d'encourager ou de soutenir financièrement le recours à ce type de technologie dans les piscines wallonnes, notamment dans le cadre des futurs investissements ou rénovations d'infrastructures sportives ? Envisagez-vous de définir, en concertation avec les gestionnaires de piscines et les autorités compétentes en matière de protection des données, un cadre ou des recommandations pour l'utilisation de l'intelligence artificielle à des fins de sécurité dans les infrastructures sportives ?

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Monsieur le Député, j'ai en effet connaissance du dispositif installé à la piscine communale de Spa. Il repose sur des caméras sous-marines ainsi que sur un système permettant d'analyser certaines situations à risque et d'envoyer une alerte aux maîtres-nageurs lorsqu'un comportement anormal est détecté.

Je veux néanmoins être très claire sur un point : cette technologie constitue une aide supplémentaire à la surveillance. Elle ne remplace évidemment ni la présence ni la vigilance des maîtres-nageurs.

Ce dispositif a été installé dans le cadre des travaux de rénovation de la piscine, soutenus financièrement par la Wallonie dans le cadre du plan Piscines. D'autres piscines wallonnes disposent également de technologies d'assistance à la surveillance. Mon administration ne dispose cependant pas, à ce stade, d'un inventaire exhaustif de l'ensemble des dispositifs installés ni d'une étude wallonne permettant de comparer objectivement l'efficacité des différentes technologies disponibles.

Les mécanismes régionaux de soutien aux infrastructures sportives permettent déjà de financer des investissements visant notamment à améliorer la sécurité des équipements. Ce type de technologie peut donc être pris en considération dans le cadre d'un projet,

en fonction de ses caractéristiques et des règles applicables.

Il faut également rester attentif aux questions liées à la protection des données dès lors que ces dispositifs reposent sur la captation et l'analyse d'images. Il appartient aux gestionnaires de respecter l'ensemble des obligations légales en la matière.

Ces innovations peuvent donc constituer un outil supplémentaire intéressant pour renforcer la sécurité dans nos piscines, mais, quelles que soient les avancées technologiques, elles doivent rester complémentaires au travail et à l'expertise des professionnels chargés de la surveillance des bassins.

Mme la Présidente. – La parole est à M. Witsel.

M. Thierry Witsel (PS). – Je remercie Mme la Ministre pour ces éléments de réponse. Je retiens surtout l'intérêt que peut représenter cette technologie qui permet de renforcer la sécurité des nageurs ainsi qu'une intervention beaucoup plus rapide en cas de noyade.

Toutefois, il est important que ces deux dimensions – sécurité et respect de la vie privée – puissent avancer de manière équilibrée dans les infrastructures sportives qui bénéficient des soutiens de la Wallonie. Je pense que ces deux paramètres sont les plus importants. Pour le reste, que l'IA vienne aider à la surveillance des maîtres-nageurs me paraît une bonne solution.

(Mme Tillieux, doyenne d'âge, prend place au fauteuil présidentiel)

Mme la Présidente. – Comme quoi, l'opposition est bien présente et assure les travaux de notre Commission.

**Question orale
de Mme Sophie Fafchamps
à Mme Jacqueline Galant, Ministre de la
Fonction publique, de la Simplification
administrative et des Infrastructures sportives,
sur « le soutien régional au projet de
développement du stade du Royal Football Club
de Liège (RFCL) »**

Mme la Présidente. – L'ordre du jour appelle la question orale de Mme Fafchamps à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sur « le soutien régional au projet de développement du stade du Royal Football Club de Liège (RFCL) ».

La parole est à Mme Fafchamps pour poser sa question.

Mme Sophie Fafchamps (Les Engagés). – Madame la Ministre, en février dernier et en février 2025, je vous ai interrogée sur les contacts menés en vue d'élaborer un plan de financement du projet de nouveau stade du Royal Football Club de Liège, qui porte le matricule 4. Pour rappel, le budget était estimé entre 20 et 30 millions d'euros pour le stade et les activités annexes.

Or, nous avons appris, la semaine dernière, que le Gouvernement avait validé, sur votre proposition, un subside de 8 millions d'euros à Ecetia afin de subventionner la construction d'une infrastructure destinée à abriter un écosystème multisports économique et médico-social dans le cadre du projet Wallonia Sport Park.

Pouvez-vous nous expliquer les raisons de ce montage ? Pourquoi passer par une intercommunale plutôt que financer directement le projet ? À combien s'élève actuellement le projet de stade ? A-t-il évolué depuis notre échange de l'année dernière ? Certains volets du projet initial seront-ils abandonnés, comme la presse en a fait écho ?

Dans quels délais l'intercommunale doit-elle vous communiquer les éléments explicitant le montage administratif, juridique et financier de ce projet ? Ce modèle de soutien à des infrastructures sportives d'ampleur pourrait-il être reproduit pour d'autres projets ?

Mme la Présidente. – La parole est à Mme la Ministre Galant.

Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives. – Madame la Députée, lors de sa séance du 17 septembre dernier, le Gouvernement a effectivement marqué son accord de principe sur l'octroi d'une subvention d'un montant maximum de 8 millions d'euros à l'intercommunale Ecetia dans le cadre du projet Wallonia Sport Park, et ce, exclusivement pour la partie sportive. Ce projet sera financé via une partie des moyens initialement prévus pour le vélodrome à Liège, ce dernier étant abandonné dans le cadre du projet de pôle sportif d'excellence multidisciplinaire de la Wallonie.

J'ai sollicité auprès d'Ecetia un dossier administratif, juridique, financier, technique et sportif en vue de l'octroi d'une promesse ferme de subvention. Ce dossier est attendu d'ici la fin de l'année 2026 afin de permettre l'engagement budgétaire du projet en 2027.

La demande de subvention a été introduite par Ecetia, intercommunale éligible aux subventions en matière d'infrastructures sportives, qui attendait un premier feu vert du Gouvernement. Le montant maximum de la subvention étant désormais connu, l'intercommunale peut à présent affiner son projet et

avancer sur la recherche de partenaires publics et privés qui feront vivre le futur Wallonia Sport Park.

Mme la Présidente. – La parole est à Mme Fafchamps.

Mme Sophie Fafchamps (Les Engagés). – Madame la Ministre, en tant que Liégeoise, je ne peux que me réjouir que l'on puisse promouvoir et accueillir un tel projet de grande envergure qui mêle sport et santé, avec un pôle social, bref, un projet global avec divers éléments. Vous n'avez pas répondu à tous les éléments de ma question, mais, comme c'est le début du dossier, j'imagine qu'il y aura encore toute une série de points à suivre. Je ne manquerai pas de revenir vers vous avec plus de questions tout au long de ce dossier.

ORGANISATION DES TRAVAUX (Suite)

Interpellations et questions orales transformées en questions écrites

Mme la Présidente. – Les questions orales de :

- Mme Fafchamps sur « l'identification des compétences numériques internes » ;
- Mme Fafchamps, sur « les standards numériques communs au Service public de Wallonie (SPW) et aux unités d'administration publique wallonnes » ;
- M. Ch. Bastin, sur « la mutualisation des outils numériques » ;
- M. Witsel, sur « le suivi du projet de rénovation du complexe sportif de Carlsbourg » ;
- M. Cloquet, sur « la vente de l'hippodrome de Wallonie » à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sont transformées en questions écrites.

Interpellations et questions orales retirées

Mme la Présidente. – Les questions orales de :

- Mme Özen, sur « l'impact de la hausse des prix des carburants sur le parc automobile du Service public de Wallonie (SPW) » ;
- Mme Özen, sur « le suivi de la réforme annoncée du télétravail au Service public de Wallonie (SPW) » ;
- Mme Özen, sur « le recyclage et la réutilisation du matériel au sein du Service public de Wallonie (SPW) » à Mme Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives, sont retirées.

Ceci clôt nos travaux de ce jour.

La séance est levée.

- La séance est levée à 19 heures 4 minutes.

LISTE DES INTERVENANTS

M. Jean-Paul Bastin, Les Engagés
Mme Phédra Clouner, Directrice générale adjointe de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB)
Mme Veronica Cremasco, Ecolo
Mme Kris Derkoningen, Commissaire à la Federal Computer Crime Unit (DJSOC/FCCU)
Mme Sophie Fafchamps, Présidente
M. Hervé Fiévet, MR
Mme Jacqueline Galant, Ministre de la Fonction publique, de la Simplification administrative et des Infrastructures sportives
M. Stéphane Guisse, Secrétaire général a.i. du Service public de Wallonie (SPW)
M. Stéphane Hazée, Ecolo
M. Julien Liradelfo, PTB
M. Vincent Maillen, MR
M. Chris Massaki Mbaki, MR
M. Jean-Luc Peeters, Directeur de la Cyber Emergency Response Team (CERT) du Centre pour la cybersécurité Belgique (CCB)
Mme Isabelle Quoilin, Conseillère en stratégie du Service public de Wallonie Digital (SPW Digital)
Mme Isabelle Roucou, Directrice générale du Service public de Wallonie Digital (SPW Digital)
Mme Éliane Tillieux, PS
M. Thierry Witsel, PS

ABRÉVIATIONS COURANTES

APD	Autorité de protection des données
BELAC	Organisme belge d'accréditation
CCB	Centre pour la cybersécurité Belgique
CEO	chief executive officer (chef de la direction, directeur général ou administrateur délégué)
CERT	Cyber Emergency Response Team (équipe d'intervention d'urgence informatique)
CORTEX	Centre régional de coordination des risques et de la transmission d'expertise
Costra	Comité stratégique du Service public de Wallonie
CRA	Cyber Resilience Act (Loi sur la cyber-résilience)
CRT	Cyber Response Team (Équipe de réponse aux cyberattaques)
CSIRT	Computer Security Incident Response Team (équipe d'intervention en cas d'incident de sécurité informatique)
DART	detection and response team (équipe de détection et d'intervention) (Microsoft)
DDoS	distributed denial of service (déné de service distribué)
DG	directeur général / direction générale
DJSOC	Directorate of Judicial Serious and Organised Crime (Direction centrale de la lutte contre la criminalité grave et organisée)
DPO	data protection officer (délégué à la protection des données)
EAP	École d'administration publique
ENISA	European Union Agency for Cybersecurity (Agence de l'Union européenne pour la cybersécurité)
ERP	Enterprise Resource Planning (planification des ressources de l'entreprise)
ESP	Electronic Stability Programm (Programme de stabilité électronique)
FCCU	Federal Computer Crime Unit (Unité fédérale de criminalité informatique)
FFA	football francophone amateur
FIFA	Fédération internationale de football association
IA	intelligence artificielle
Infrasports	Direction des infrastructures sportives
IP	Internet protocol
ISO	International Organization for Standardization (Organisation internationale de normalisation)
IT	information technology (technologies de l'information)
LCCU	local computer crime unit (unité(s) locale(s) de criminalité informatique)
MET	Ministère de l'Équipement et des Transports
MFA	multi-factor authentication (authentification multifacteurs)
NIS	Directive on Security of Network and Information Systems (Directive sur la sécurité des réseaux et des systèmes d'information)
OIP	organisme(s) d'intérêt public
OT	operational technology (technologie opérationnelle)
PC	personal computer (ordinateur personnel, micro-ordinateur, ordinateur individuel)
RCCU	regional computer crime unit (unité(s) régionale(s) de criminalité informatique)
RFCL	Royal Football Club de Liège
RGPD	Règlement général sur la protection des données
RH	ressources humaines
SAP	Systems, Applications and Products for data processing (Systèmes, applications et produits pour le traitement de données)
SMS	short message service (service de messages courts, texto)
SOC	security operation center (centre des opérations de sécurité)
SPA	single-page application (application web accessible via une page web unique)
SPW	Service public de Wallonie
UAP	unité(s) d'administration publique
USB	Universal Serial Bus (bus universel en série)
VPN	virtual private network (réseau virtuel privé)
WBFIn	décret portant organisation du budget et de la comptabilité des services du Gouvernement wallon